Part No. 209570-C
November 2001

4401 Great America Parkway
Santa Clara, CA 95054

Using Web-based Management for the Business Policy Switch 2000 Software Version 2.0

Nortel Networks™

Copyright © 2001 Nortel Networks

All rights reserved. November 2001.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks NA Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Autotopology, BaySecure, BayStack, Business Policy Switch, Nortel Networks, the Nortel Networks logo, Optivity, and Optivity Policy Services are trademarks of Nortel Networks.

Internet Explorer, Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Acrobat and Adobe are registered trademarks of Adobe Systems Incorporated.

Netscape Navigator is a registered trademark of Netscape Communications Corporation.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

USA requirements only

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

European requirements only

EN 55 022 statement

This is to certify that the Nortel Networks Business Policy Switch 2000 is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class A (CISPR 22).

Warning: This is a Class A product. In a domestic environment, this product may cause radio interference, in which case, the user may be required to take appropriate measures.

Achtung: Dieses ist ein Gerät der Funkstörgrenzwertklasse A. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Attention: Ceci est un produit de Classe A. Dans un environnement domestique, ce produit risque de créer des interférences radioélectriques, il appartiendra alors à l’utilisateur de prendre les mesures spécifiques appropriées.

AEC Declaration of Conformity

This product conforms (or these products conform) to the provisions of the R&TTE Directive 1999/5/EC.

Japan/Nippon requirements only

Voluntary Control Council for Interference (VCCI) statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwan requirements

Bureau of Standards, Metrology and Inspection (BSMI) Statement

警告使用者:

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策.

Canada requirements only

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Business Policy Switch 2000) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (Business Policy Switch 2000) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABLITITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. Limitation of Remedies. IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER’S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. General

a) If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-Odd entities) and 48 C.F.R. 227.7202 (for Odd entities).

b) Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

c) Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer’s use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

d) Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

e) The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

f) This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Preface 25

Before you begin 25
Text conventions 26
Related publications 26
How to get help 28

Chapter 1
Using the Web-based management interface 29

New features 29
Stacking compatibility 30
Software version 2.0 compatibility with BayStack 450 switches 32
Requirements 33
Port numbering syntax 33
Logging in to the Web-based management interface 34
Web page layout 35
    Menu 36
    Management page 39

Chapter 2
Administering the switch 41

Viewing general information 41
    Viewing system information 42
    Viewing CPU and memory utilization 43
Configuring system security 44
    Setting console, Telnet, and Web passwords 44
    Configuring RADIUS security 46
Logging on to the management interface 47
Resetting the BPS 2000 49

Resetting the BPS 2000 to system defaults 50
Logging out of the management interface 51

Chapter 3
Viewing summary information 53

Viewing stack information 53
Viewing summary switch information 55
Viewing switch information in real time 57
Changing stack numbering 60
Identifying unit numbers 62

Chapter 4
Configuring the switch 63

Configuring BootP, IP, and gateway settings 64
Modifying system settings 67
About SNMP 68
Configuring SNMPv1 69
Configuring SNMPv3 70
  Viewing SNMPv3 system information 70
  Configuring user access to SNMPv3 72
    Creating an SNMPv3 system user configuration 72
    Deleting an SNMPv3 system user configuration 75
  Configuring an SNMPv3 system user group membership 75
    Mapping an SNMPv3 system user to a group 75
    Deleting an SNMPv3 group membership configuration 77
  Configuring SNMPv3 group access rights 78
    Creating an SNMPv3 group access rights configuration 78
    Deleting an SNMPv3 group access rights configuration 79
  Configuring an SNMPv3 management information view 80
    Creating an SNMPv3 management information view configuration 80
    Deleting an SNMPv3 management information view configuration 82
  Configuring an SNMPv3 system notification entry 82
    Creating an SNMPv3 system notification configuration 83
    Deleting an SNMPv3 system notification configuration 84
  Configuring an SNMPv3 management target address 85

        - Creating an SNMPv3 target address configuration 85
        - Deleting an SNMPv3 target address configuration 87
    - Configuring an SNMPv3 management target parameter 87
        - Creating an SNMPv3 target parameter configuration 87
        - Deleting an SNMPv3 target parameter configuration 89
- Configuring SNMP traps 89
        - Creating an SNMP trap receiver configuration 89
        - Deleting an SNMP trap receiver configuration 90
- Configuring EAPOL-based security 91
- Managing remote access by IP address 94
- Configuring MAC address-based security 96
    - Configuring MAC address-based security 97
    - Configuring ports 99
    - Adding MAC addresses 102
    - Clearing ports 103
    - Enabling security on ports 104
    - Deleting ports 105
    - Filtering MAC destination addresses 106
    - Deleting MAC DAs 107
- Viewing learned MAC addresses by VLAN 108
- Locating a specific MAC address 109
- Configuring port’s autonegotiation, speed, duplex, status, and alias 111
- Configuring high speed flow control 114
- Downloading switch images 116
    - Observing LED indications 118
    - Upgrading software 119
        - Upgrading software in a Pure BPS 2000 stack or a standalone BPS 2000 . 120
        - Upgrading software in a Hybrid stack 121
- Storing and retrieving a switch configuration file from a TFTP server 124
- Configuring port communication speed 127
- Setting system operational modes 128

Chapter 5
Configuring remote network monitoring (RMON). 129

- Configuring RMON fault threshold parameters 130

  - Creating an RMON fault threshold 130
  - Deleting an RMON threshold configuration 132
- Viewing the RMON fault event log 133
- Viewing the system log 134
- Viewing RMON Ethernet statistics 136
  - Viewing RMON Ethernet statistics in a bar graph format 138
  - Viewing RMON Ethernet statistics in a pie chart format 139
- Viewing RMON history 140
  - Viewing RMON statistics in a line graph format 142

Chapter 6
Viewing system statistics 143

- Viewing port statistics 143
  - Zeroing ports 146
  - Viewing port statistics in a pie chart format 147
  - Viewing port statistics in a bar graph format 147
- Viewing all port errors 148
- Viewing interface statistics 150
  - Viewing interface statistics in a pie chart format 152
  - Viewing interface statistics in a bar graph format 152
- Viewing Ethernet error statistics 153
  - Viewing Ethernet error statistics in a pie chart format 155
  - Viewing Ethernet error statistics in a bar graph format 156
- Viewing transparent bridging statistics 157
  - Viewing transparent bridging statistics in a pie chart format 159
  - Viewing transparent bridging statistics in a bar graph format 160

Chapter 7
Configuring application settings 161

- Configuring port mirroring 162
- Configuring rate limiting 165
- Configuring IGMP 167
- Viewing Multicast group membership configurations 169
- Creating and managing virtual LANs (VLANs) 171
  - Port-based VLANs 172

Protocol-based VLANs 172

MAC SA-based VLANs 172

Configuring VLANs 173

Creating a port-based VLAN 175

Modifying a port-based VLAN 176

Creating a protocol-based VLAN 178

Modifying a protocol-based VLAN 182

Creating a MAC SA-based VLAN 183

Modifying a MAC SA-based VLAN 185

Selecting a management VLAN 187

Deleting a VLAN configuration 188

Configuring broadcast domains 188

Viewing VLAN port information 190

Managing spanning tree groups 192

Creating spanning tree groups 193

Associating STG with VLAN membership 195

Configuring ports for spanning tree 197

Changing spanning tree bridge switch settings 199

Configuring MultiLink Trunk (MLT) members 202

Monitoring MLT traffic 205

Chapter 8
Implementing QoS Using QoS Wizard and QoS Quick Config 207

Using QoS Wizard 208

Configuring Standard traffic with the QoS Wizard 208

Prioritizing traffic with the QoS Wizard 210

Prioritizing VLANs with the QoS Wizard 213

Prioritizing IP applications with the QoS Wizard 220

Prioritizing user defined flows with the QoS Wizard 226

Using QoS Quick Config 236

Using QoS Quick Config to configure interface groups 237

Using QoS Quick Config to configure policies 239

Configuring QoS Quick Config filters 241

Deleting Qos Quick Config filters from the filter group 246

Configuring QoS Quick Config meters 247
Configuring QoS Quick Config shapers 248
Configuring QoS Quick Config policies 250

Chapter 9
Implementing QoS using QoS Advanced 253

Configuring an interface group 254
    Creating an interface group configuration 254
    Displaying Interface ID Table 257
    Adding or removing interface group members 258
    Deleting an interface group configuration 260
Configuring 802.1p priority queue assignment 261
Configuring 802.1p priority mapping 263
Creating a DSCP queue assignment 264
Configuring DSCP mapping 265
IP filter and IP filter group configurations 268
    Creating an IP filter configuration 268
    Deleting an IP filter configuration 272
    Creating an IP filter group configuration 272
    Modifying an IP filter group configuration 275
    Deleting an IP filter group configuration 277
Layer 2 filter and layer 2 filter group configurations 278
    Creating a layer 2 filter configuration 278
    Deleting a layer 2 filter configuration 283
    Creating a layer 2 filter group configuration 284
    Modifying a layer 2 filter group configuration 286
    Deleting a layer 2 filter group configuration 287
Configuring QoS actions 288
    Creating a filter action configuration 288
    Deleting an action configuration 290
Configuring QoS meters 291
    Creating a meter 291
    Viewing meters 293
    Deleting a meter 294
Configuring QoS shapers 294

- Creating a shaper . . . 294
- Viewing shapers . . . 296
- Deleting a shaper . . . 297

Configuring QoS policies . . . 297

- Installing defined filters . . . 298
- Viewing hardware policy statistics . . . 301
- Deleting a hardware policy configuration . . . 303

Configuring QoS Policy Agent (QPA) characteristics . . . 304

Chapter 10
Implementing Common Open Policy Services (COPS). . . . 307

Viewing COPS statistics and capabilities . . . 308

Creating a COPS configuration . . . 311

- Deleting a COPS client configuration . . . 314

Chapter 11
Support menu. . . . 315

Using the online help option . . . 315

Downloading technical publications . . . 316

Upgrade option . . . 317

Index . . . 319

Figures

Figure 1 Web-based management interface home page 35
Figure 2 Web page layout 36
Figure 3 Console page 39
Figure 4 System Information home page 42
Figure 5 CPU/Memory Utilization page 43
Figure 6 Console password setting page 45
Figure 7 RADIUS page 46
Figure 8 Web-based management interface log on page 47
Figure 9 System Information home page 48
Figure 10 Reset page 49
Figure 11 Reset to Default page 50
Figure 12 Stack Information page 54
Figure 13 Switch Information page 55
Figure 14 Switch View page 57
Figure 15 Stack Numbering Setting page 60
Figure 16 Identify Unit Numbers page 62
Figure 17 IP page for a standalone BPS 2000 64
Figure 18 IP page for a stack 65
Figure 19 System page 67
Figure 20 SNMPv1 page 69
Figure 21 System Information page 71
Figure 22 User Specification page 73
Figure 23 Group Membership page 76
Figure 24 Group Access Rights page 78
Figure 25 Management Information View page 81
Figure 26 Notification page 83
Figure 27 Target Address page 85
Figure 28 Target Parameter page 88
Figure 29 SNMP Trap Receiver page 90

Figure 30 EAPOL Security Configuration page (1 of 2) 92
Figure 31 EAPOL Security Configuration page (2 of 2) 92
Figure 32 Remote Access page 95
Figure 33 Security Configuration page 98
Figure 34 Port Lists page 100
Figure 35 Port List View, Port List page 101
Figure 36 Port List View, Learn by Ports page 101
Figure 37 Security Table page 102
Figure 38 Port List View, Clear by Ports page 104
Figure 39 Port Configuration page 105
Figure 40 DA MAC Filtering page 106
Figure 41 MAC Address Table page 108
Figure 42 Find MAC Address Table page 110
Figure 43 Port Management page 112
Figure 44 High Speed Flow Control page 115
Figure 45 Software Download page for a Pure BPS 2000 stack 116
Figure 46 Software Download page for a Hybrid stack 117
Figure 47 Configuration File Download/Upload page 124
Figure 48 Console/Communication Port page 127
Figure 49 Stack Operational Mode page 128
Figure 50 RMON Threshold page 130
Figure 51 RMON Event Log page 133
Figure 52 System Log page 134
Figure 53 RMON Ethernet page 136
Figure 54 RMON Ethernet: Chart in a bar graph format 138
Figure 55 RMON Ethernet: Chart in a pie chart format 139
Figure 56 RMON History page 140
Figure 57 Port page 144
Figure 58 Port: Chart page in a pie chart format 147
Figure 59 Port: Chart page in a bar graph format 148
Figure 60 Port Error Summary page 149
Figure 61 Interface page 150
Figure 62 Interface: Chart in a pie chart format 152
Figure 63 Interface: Chart in a bar graph format 153
Figure 64 Ethernet Errors page 154

Figure 65 Ethernet Error: Chart in a pie chart format 156
Figure 66 Ethernet Error: Chart in a bar graph format 157
Figure 67 Transparent Bridging page 158
Figure 68 Transparent Bridging: Chart in a pie chart format 159
Figure 69 Transparent Bridging: Chart in a bar graph format 160
Figure 70 Port Mirroring page 162
Figure 71 Rate Limiting page 165
Figure 72 IGMP Configuration page 167
Figure 73 IGMP: VLAN Configuration page 168
Figure 74 IGMP Multicast Group Membership page 170
Figure 75 VLAN Configuration page 173
Figure 76 VLAN Configuration: Port Based setting page 175
Figure 77 VLAN Configuration: Port Based modification page 176
Figure 78 VLAN Configuration: Protocol Based setting page 178
Figure 79 VLAN Configuration: Protocol Based modification page 182
Figure 80 VLAN Configuration: MAC SA Based setting page 184
Figure 81 VLAN Configuration: MAC SA Based modification page 185
Figure 82 VLAN Configuration: MAC Address page 186
Figure 83 Port Configuration page 189
Figure 84 Port Information page 191
Figure 85 Spanning Tree Group Configuration page 193
Figure 86 Spanning Tree VLAN Membership page 195
Figure 87 Spanning Tree Add VLAN page 196
Figure 88 Spanning Tree Remove VLAN page 196
Figure 89 Spanning Tree Port Configuration page 197
Figure 90 Spanning Tree Bridge Information page 199
Figure 91 Group page 203
Figure 92 Utilization page 205
Figure 93 QoS Wizard opening page 209
Figure 94 Packet prioritization selection page 209
Figure 95 Standard prioritization page 210
Figure 96 Session confirmation page 210
Figure 97 QoS Policies to Configure window 212
Figure 98 Packet prioritization explanation page 213
Figure 99 VLAN prioritization selection page 214

Figure 100 Meter for VLAN page 214
Figure 101 Meter setting for VLAN page 215
Figure 102 Service Class selection for VLAN page 216
Figure 103 Shaper for VLAN page 217
Figure 104 Setting shaping parameters for VLAN page 218
Figure 105 Additional VLANs page 219
Figure 106 Packet prioritization page with prioritized VLAN(s) 220
Figure 107 QoS Policies to Configure window with VLAN entry 220
Figure 108 IP Application prioritization page 221
Figure 109 Meter for IP Application page 221
Figure 110 Meter setting for IP Application page 222
Figure 111 Service Class selection for IP Application page 223
Figure 112 Shaper for IP Application page 224
Figure 113 Setting shaping parameters for IP Application page 225
Figure 114 Packet prioritization page with prioritized IP Application(s) 226
Figure 115 QoS Policies to Configure window with IP Application entry 226
Figure 116 Policy label page 227
Figure 117 Policy definition page 227
Figure 118 IP classification rules page (1 of 2) 228
Figure 119 IP classification rules page (2 of 2) 228
Figure 120 Layer 2 classification rules page (1 of 2) 229
Figure 121 Layer 2 classification rules page (2 of 2) 230
Figure 122 Meter for user defined flow page 231
Figure 123 Meter setting for user defined flow page 231
Figure 124 Service Class selection for user defined flow page 232
Figure 125 Shaper for user defined flow page 233
Figure 126 Setting shaping parameters for user defined flow page 234
Figure 127 Additional user defined flows page 235
Figure 128 Packet prioritization page with prioritized User Defined Flow(s) 236
Figure 129 QoS Policies to Configure window with user defined flow entry 236
Figure 130 QoS Quick Config Interface Group page—View Interface Group 237
Figure 131 QoS Quick Config Interface Group page—Create Interface Group 238
Figure 132 QoS Quick Config Interface Group page—View Interface Group 239
Figure 133 QoS Quick Config Policy page (1 of 3) 240
Figure 134 QoS Quick Config Policy page (2 of 3) 240

Figure 135 QoS Quick Config Policy page (3 of 3) 241
Figure 136 QoS Quick Config page for configuring IP filters page (1 of 2) 242
Figure 137 QoS Quick Config page for configuring IP filters page (2 of 2) 242
Figure 138 QoS Quick Config page for configuring layer 2 filters page (1 of 2) 244
Figure 139 QoS Quick Config page for configuring layer 2 filters page (2 of 2) 244
Figure 140 QoS Quick Config page with existing filter group choice 246
Figure 141 QoS Quick Config Policy page with displayed filter group 247
Figure 142 QoS Quick Config Policy page with expanded meter area 248
Figure 143 Step 3: Shaper 249
Figure 144 Shaper box 249
Figure 145 Policy area of QoS Quick Config Policy page 251
Figure 146 QoS Advanced Policies page with configured policies (1 of 2) 252
Figure 147 QoS Advanced Policies page with configured policies (2 of 2) 252
Figure 148 QoS Advanced Interface Configuration page 255
Figure 149 Interface ID page 258
Figure 150 Interface Group Assignment page 259
Figure 151 802.1p Priority Queue Assignment page 262
Figure 152 802.1p Priority Mapping page 263
Figure 153 DSCP Queue Assignment page 264
Figure 154 DSCP Mapping Table page 266
Figure 155 DSCP Mapping Modification page 267
Figure 156 IP Classification page (1 of 3) 268
Figure 157 IP Classification page (2 of 3) 269
Figure 158 IP Classification page (3 of 3) 269
Figure 159 IP Classification Group page 274
Figure 160 Layer2 Classification page (1 of 2) 278
Figure 161 Layer2 Classification page (2 of 2) 279
Figure 162 Layer2 Group page 285
Figure 163 Layer2 Group modification page 286
Figure 164 Action page 289
Figure 165 QoS Advanced Meter page 292
Figure 166 QoS Advanced Shapers page 295
Figure 167 QoS Advanced Policies page (1 of 3) 298
Figure 168 QoS Advanced Policies page (2 of 3) 299
Figure 169 QoS Advanced Policies page (3 of 3) 299

Figure 170 Policy Statistics page 302
Figure 171 Agent page (1 of 2) 304
Figure 172 Agent page (2 of 2) 305
Figure 173 Status page 308
Figure 174 Configuration page 312
Figure 175 Online help window 316
Figure 176 Nortel Networks Technical Documentation Web site 317
Figure 177 Nortel Networks Customer Support Web site 318

Tables

Table 1 Main headings and options 37
Table 2 Menu icons 38
Table 3 Page buttons and icons 40
Table 4 System Information page items 43
Table 5 CPU/Memory Utilization page items 44
Table 6 Console page items 45
Table 7 RADIUS page items 46
Table 8 User levels and access levels 48
Table 9 Stack Information page fields 54
Table 10 Switch Information page fields 56
Table 11 BPS 2000 switch LED descriptions 58
Table 12 Stack Numbering Setting page fields 60
Table 13 IP page items 65
Table 14 System page items 68
Table 15 SNMPv1 page items 70
Table 16 System Information section fields 71
Table 17 SNMPv3 Counters section fields 72
Table 18 User Specification Table section items 73
Table 19 User Specification Creation section items 74
Table 20 Group Membership page items 76
Table 21 Group Access Rights page items 79
Table 22 Management Information View page items 81
Table 23 Notification page items 83
Table 24 Target Address page items 86
Table 25 Target Parameter page items 88
Table 26 SNMP Trap Receiver page items 90
Table 27 EAPOL Security Configuration page fields 93
Table 28 Remote Access page fields 95
Table 29 Security Configuration page items 98

Table 30 Ports Lists page items 100
Table 31 Security Table page items 103
Table 32 Port Configuration page items 105
Table 33 DA MAC Filtering page items 106
Table 34 MAC Address Table page items 109
Table 35 Port Management page items 113
Table 36 High Speed Flow Control page items 115
Table 37 Software Download page items 117
Table 38 LED Indications during the software download process 118
Table 39 Configuration File page items 125
Table 40 Requirements for storing or retrieving configuration parameters on a TFTP server 126
Table 41 Parameters not saved to the configuration file 126
Table 42 Console/Communication Port Setting page items 127
Table 43 Stack Operational Mode page items 128
Table 44 RMON Threshold page items 131
Table 45 RMON Event Log page fields 134
Table 46 System Log page fields 135
Table 47 RMON Ethernet page items 136
Table 48 RMON History page items 141
Table 49 Port page items 144
Table 50 Port Error Summary Table fields 149
Table 51 Interface page items 151
Table 52 Ethernet Errors page items 154
Table 53 Transparent Bridging page items 158
Table 54 Port Mirroring page items 163
Table 55 Port-based monitoring modes 164
Table 56 Address-based monitoring modes 164
Table 57 Rate Limiting page items 166
Table 58 IGMP Configuration page items 167
Table 59 IGMP: VLAN Configuration page items 168
Table 60 IGMP Multicast Group Membership page items 170
Table 61 VLAN Configuration page items 174
Table 62 VLAN Configuration: Port Based setting page items 175
Table 63 VLAN Configuration: Port Based modification page items 177

Table 64 VLAN Configuration: Protocol Based setting page items 179
Table 65 Standard protocol-based VLANs and PID types 180
Table 66 Predefined Protocol Identifier (PID) 181
Table 67 VLAN Configuration: Protocol Based modification page items 183
Table 68 VLAN Configuration: MAC SA Based setting page items 184
Table 69 VLAN Configuration: MAC SA Based modification page items 186
Table 70 Port Configuration page items 189
Table 71 Port Information page items 191
Table 72 Spanning Tree Group Configuration page items 193
Table 73 Spanning Tree Port Configuration page items 198
Table 74 Spanning Tree Bridge Information page items 200
Table 75 Group page items 204
Table 76 Utilization page items 205
Table 77 QoS Interface Queue Table section items 255
Table 78 Interface Group Table section items 256
Table 79 Interface Group Creation section page items 257
Table 80 Interface ID page items 258
Table 81 Interface Group Assignment page items 259
Table 82 802.1p Priority Assignment Table section page items 262
Table 83 802.1p Priority Mapping page items 264
Table 84 DSCP Queue Assignment page items 265
Table 85 DSCP Mapping Table page items 266
Table 86 DSCP Mapping Modification page items 267
Table 87 IP Filter Table and Filter Creation sections page items 270
Table 88 IP Filter Group section page items 273
Table 89 IP Classification Group page items 274
Table 90 IP Modification Group page items 276
Table 91 Layer2 Filter Table and Layer2 Filter Creation section items 279
Table 92 IP Filter Group Table section items 284
Table 93 Layer2 Group page items 285
Table 94 Layer2 Group modification page items 287
Table 95 Action page items 289
Table 96 Meter Creation fields 292
Table 97 Meter Table fields 293
Table 98 Shaper Creation fields 295

Table 99 Shaper Table fields 296
Table 100 Policy page items 300
Table 101 Policy Statistics page items 302
Table 102 Agent page items 305
Table 103 Status page items 308
Table 104 COPS Configuration Table section items 312

Preface

Welcome to *Using Web-based Management for the Business Policy Switch 2000 Software Version 2.0*. This document provides instructions on configuring and managing the Business Policy Switch 2000* through the World Wide Web.

The Web-based management interface is one of many tools specifically designed to assist the network manager in creating complex standalone or network configurations. In addition to the Web-based management system discussed in this book, you can manage the BPS 2000 using SNMP, the Command Line Interface (CLI), Device Manager (DM), or the console interface (CI) menus. Refer to the documents listed "Related publications" on page 26 for information on using and managing the BPS 2000.

This guide describes how to use the Web-based management user interface to configure and maintain your BPS 2000 and the devices connected within its framework.

Before you begin

This guide is intended for network managers who are responsible for configuring BPS 2000. Consequently, this guide assumes prior knowledge and understanding of the terminology, theories, and practices and specific knowledge about the networking devices, protocols, and interfaces that comprise your network.

You should have working knowledge of the Windows* operating system, graphical user interfaces (GUIs), and Web browsers.

Text conventions

This guide uses the following text conventions:

italic text	Indicates new terms and book titles.
separator (>)	Shows menu paths. Example: Configuration > Port Management identifies the Port Management option on the Configuration menu.

Related publications

For more information about using the Web-based management user interface and the BPS 2000, refer to the following publications:

- *Release Notes for the Business Policy Switch 2000 Software Version 2.0* (part number 210676-F)

  Documents important changes about the software and hardware that are not covered in other related publications.
- *Using the Business Policy Switch 2000 Software Version 2.0* (part number 208700-C)

  Describes how to use the BPS 2000.
- *Business Policy Switch 2000 Installation Instructions* (part number 209319-A*)*

  Describes how to install the BPS 2000.
- *Reference for the Business Policy Switch 2000 Command Line Interface Software Version 2.0* (part number 212160-B)

  Describes how to use the Command Line Interface (CLI) to configure and manage the BPS 2000.
- *Reference for the Business Policy Switch 2000 Management Software Version 2.0* (part number 209322-C)

Describes how to use the Java Device Manager to configure and manage the BPS 2000.

- *Installing Media Dependent Adapters (MDA)s* (part number 302403-H)

  Describes how to install optional MDAs in your Business Policy Switch 2000.

- *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters* (part number 312865-B)

  Describes how to install optional GBICs and SFP GBICs into the optional MDA in your Business Policy Switch 2000.

- *Installing Optivity Policy Services* (part number 306972-E Rev 00)

  Describes how to install Optivity Policy Services*.

- *Managing Policy Information in Optivity Policy Services* (part number 306969-F Rev 00)

  Describes how to configure and manage Optivity Policy Services.

- *Release Notes for Optivity Policy Services Version 2.0.1* (part number 306975-F Rev 00)

  Documents important Optivity Policy Services changes that are not covered in other related publications.

- *Task Map - Installing Optivity Policy Services Product Family* (part number 306976-E Rev 00)

  Provides a quick map to installing Optivity Policy Services.

- *Known Anomalies for Optivity Policy Services Version 2.0* (part number 306974-E Rev 00)

  Describes known anomalies with Optivity Policy Services.

You can print selected technical manuals and release notes free, directly from the Internet. Go to the www.nortelnetworks.com/documentation URL. (The product family for the BPS 2000 is Data and Internet.) Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe* Acrobat Reader* to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to Adobe Systems at the www.adobe.com URL to download a free copy of the Adobe Acrobat Reader.

Additionally, you can obtain printed books from Fatbrain.com. Contact Fatbrain.com to order a printed book at http://www1.fatbrain.com/documentation/nortel.

How to get help

If you purchased a service contract for your Nortel Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Nortel Networks service program, contact one of the following Nortel Networks Technical Solutions Centers:

Technical Solutions Center	Telephone
Europe, Middle East, and Africa	(33) (4) 92-966-968
North America	(800) 4NORTEL or (800) 466-7835
Asia Pacific	(61) (2) 9927-8800
China	(800) 810-5000

Additional information about the Nortel Networks Technical Solutions Centers is available from the www.nortelnetworks.com/help/contact/global URL.

An Express Routing Code (ERC) is available for many Nortel Networks products and services. When you use an ERC, your call is routed to a technical support person who specializes in supporting that product or service. To locate an ERC for your product or service, go to the http://www130.nortelnetworks.com/cgi-bin/eserv/common/essContactUs.jsp URL.

Chapter 1
Using the Web-based management interface

This chapter describes the requirements for using the Web-based management interface and how to use it as a tool to configure your BPS 2000. This chapter covers:

- "New features," next
- "Stacking compatibility" on page 30
- "Software version 2.0 compatibility with BayStack 450 switches" on page 32
- "Requirements" on page 33
- "Port numbering syntax" on page 33
- "Logging in to the Web-based management interface" on page 34
- "Web page layout" on page 35

New features

The following new features that you can access through Web-based management have been introduced to the BPS 2000 software since version 1.0:

- Introduced with software version 2.0
    - Support for BPS 2000-1GT, BPS 2000-2GT, and BPS 2000-2GE MDAs (refer to *Installing Media Dependent Adapters (MDA)s* and *Installing Gigabit Interface Converters and Small Form Factor Pluggable Interface Converters*)
    - Ability to view CPU and memory utilization (refer to Chapter 2)
    - Ability to set per port spanning tree path cost and priority (refer to Chapter 7)
    - Shaping for QoS networks (refer to Chapters 8 and 9)
    - Improved QoS Wizard (refer to Chapter 8)

  - QoS Quick Config (refer to Chapter 8)
  - Port naming (refer to Chapter 4)
  - MAC address-based filtering (refer to Chapter 4)
  - Individual IP addresses for each unit in the stack (refer to Chapter 4)
  - Configurable VID for tagged BPDU with multiple spanning tree groups (refer to Chapter 7)
  - Specifying multiple VLANs in a QoS single filter (refer to Chapters 8 and 9)
- Introduced with software version 1.2
  - VLANS increased to 256
  - Support for multiple spanning tree groups (refer to Chapter 7)
  - IP manager list (refer to Chapter 4)
- Introduced with software version 1.1
  - QoS metering added to policy-enabled networks (refer to Chapter 8)
  - Support for the BayStack 450-1GBIC MDA
  - EAPOL-based security (refer to Chapter 4)
  - Automatic PVID (refer to Chapter 5)
  - Table of port statistics (refer to Chapter 6)

➡ **Note:** To access the software version 2.0 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Stacking compatibility

You can stack the BPS 2000 up to 8 units high. There are two types of stacks:

- Pure BPS 2000—This stack has *only* BPS 2000 switches. It is sometimes referred to as a pure stack. The stack operational mode for this type of stack is Pure BPS 2000 Mode.

- Hybrid—This stack has a combination of BPS 2000 switches *and* BayStack* 450 and/or BayStack 410 switches. It is sometimes referred to as a mixed stack. The stack operational mode for this type of stack is Hybrid Mode.

When you work with the BPS 2000 in standalone mode, you should ensure that the stack operational mode shows Pure BPS 2000 Mode, and does not show Hybrid Mode.

All BPS 2000 switches in the stack must be running the identical version of software, and all the BayStack switches must be running the identical version of software.

When you are working with a mixed stack, you *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for the BayStack 450 switch and BayStack 410 switch must have the same ISVN as the BPS 2000. If the ISVNs are not the same, the stack does not operate.

In sum, the stacking software compatibility requirements are as follows:

- Pure BPS 2000 stack—All units must be running the same software version.
- Pure BayStack 450 stack—All units must be running the same software version.
- Hybrid stack:
  - All BPS 2000 units must be running the same software version.
  - All BayStack 410 units must be running the same software version.
  - All BayStack 450 units must be running the same software version.
  - All software versions must have the identical ISVN.

Refer to Appendix B of *Using the Business Policy Switch 2000 Software Version 2.0* for complete information on interoperability and compatibility between the BPS 2000 and BayStack switches.

Software version 2.0 compatibility with BayStack 450 switches

The BPS 2000 software version 2.0 is compatible with BayStack 450 software version 4.1.

When you are using a local console to access the BPS 2000 software version 2.0 features with a Hybrid, or mixed, stack (BPS 2000 and BayStack 450 and 410 switches in the same stack), you must plug your local console into a BPS 2000 unit.

To find out which version of the BPS 2000 software is running, use the console interface (CI) menus or the Web-based management system:

- CI menus—From the main menu of the console, choose Systems Characteristics menu. The software currently running is displayed in sysDescr.
- Web-based management system—Open the System Information page, which is under Administration on the main menu. The software currently running is displayed in the sysDescription field.

You can use 256 port-, protocol-, and MAC SA-based VLANs for the stack with a Pure BPS 2000 stack running software version 1.2. (The maximum number of MAC SA-based VLANs available is 48). If you are working with a mixed, or Hybrid, stack, you can use 64 VLANs for the entire stack. When you change from a Pure BPS 2000 Stack mode to a Hybrid Stack mode:

- If you have up to 64 VLANs on the Pure BPS 2000 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS 2000 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

Also, a mixed, or Hybrid, stack does not support multiple Spanning Tree Groups (STG). You have a single instance of STG when working with a mixed stack.

- If you have up to 64 VLANs on the Pure BPS 2000 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS 2000 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

Also, a mixed, or Hybrid, stack does not support multiple Spanning Tree Groups (STG). You have a single instance of STG when working with a mixed stack.

➡ **Note:** Refer to *Using the Business Policy Switch 2000 Software Version 2.0* for complete information on upgrading software for a Pure BPS2000 stack and for a Hybrid stack.

Requirements

To use the Web-based management interface, you need the following items:

- A recent computer connected to any of the network ports
- One of the following Web browsers installed on the computer (check the memory requirements):
  - Microsoft Internet Explorer*, version 4.0 or later (Windows 95/98/NT)
  - Netscape Navigator*, version 4.51 or later (Windows 95/98/NT & Unix)
- The IP address of the BPS 2000
- A web browser optimized for 800 by 600 pixel screen size

➡ **Note:** The Web-based management interface Web pages may load at different speeds depending on the Web browser you use.

Port numbering syntax

When you enter a port number in a stack configuration, you must specify a unit/port number. A unit/port number consists of the unit number, a slash (/), and the port number. For example, 1/1 is the unit number 1 and port number 1, and 3/11 is unit number 3 and port number 11.

In some cases, you can use a list of ports, or a port list. In this case, the same unit/port number notation applies. In addition, you can use hyphens to specify ranges of ports. For example, 1/1-7,2/1-7,2/9,3/1-4,4/12 is a valid unit/port number list. It represents the following port order:

- Unit 1: ports 1 to 7
- Unit 2: ports 1 to 7 and port 9
- Unit 3: ports 1 to 4
- Unit 4: port 12

Logging in to the Web-based management interface

Before you log in to the Web-based management interface, use the console interface to verify the VLAN port assignments and to ensure that your switch CPU and your computer are assigned to the same VLAN. If the devices are not connected to the same VLAN, you cannot access the Web-based management system.

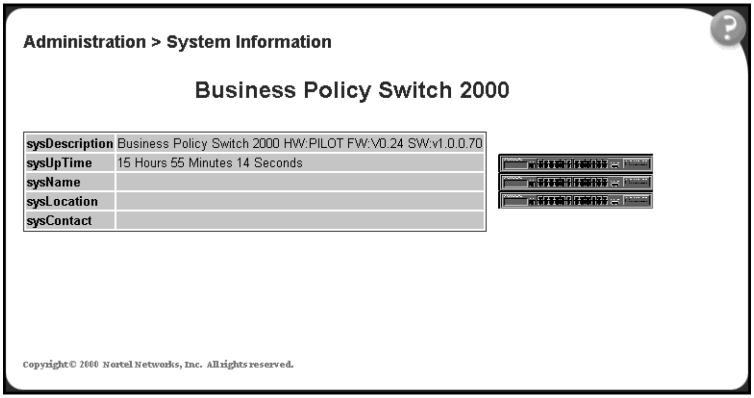
To log in to the Web-based management interface, follow these steps:

1 Start your Web browser.

2 In the Web address field, enter the IP address for your host switch or stack, for example, http://10.30.31.105, and press [Enter].

The home page opens (Figure 1).

Figure 1 Web-based management interface home page



Administration > System Information

Business Policy Switch 2000

sysDescription	Business Policy Switch 2000 HW:PILOT FW:V0.24 SW:v1.0.0.70
sysUpTime	15 Hours 55 Minutes 14 Seconds
sysName	
sysLocation	
sysContact	

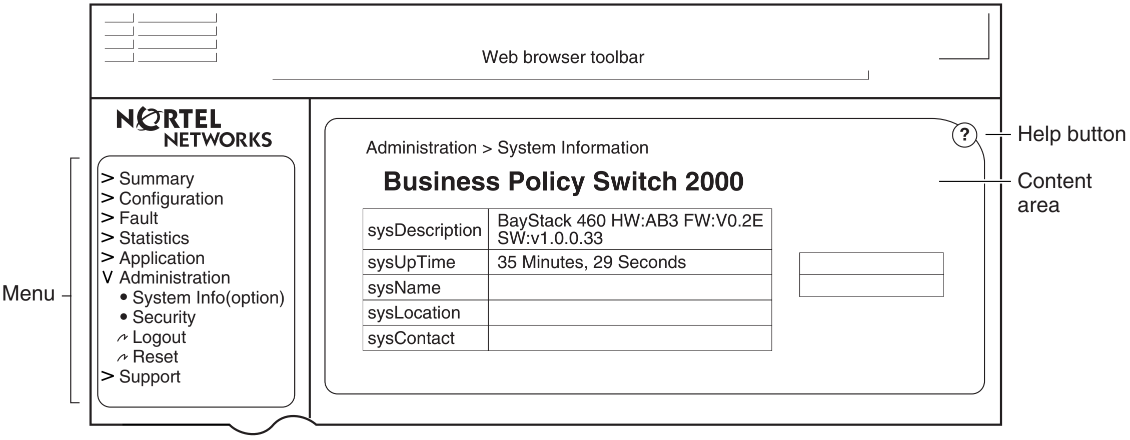
Copyright© 2000 Nortel Networks, Inc. All rights reserved.

Network security does not yet exist the first time you access the Web-based management user interface. As the system administrator, you must create access parameters and passwords to protect the integrity of your network configuration(s). For more information on setting access parameters and system passwords, refer to Chapter 4.

Web page layout

The home Web page (Figure 2) and all successive Web pages have a common layout. Each is divided into two sections: the menu and the management page. All Web pages are optimized for a 800 x 600 pixel screen size.

Figure 2 Web page layout


Web browser toolbar
NORTEL NETWORKS
Menu
> Summary
> Configuration
> Fault
> Statistics
> Application
V Administration
• System Info(option)
• Security
Logout
Reset
> Support
Help button
Content area
?
9794EA

Administration > System Information

Business Policy Switch 2000

sysDescription	BayStack 460 HW:AB3 FW:V0.2E SW:v1.0.0.33
sysUpTime	35 Minutes, 29 Seconds
sysName	
sysLocation	
sysContact	

Menu

The menu, as shown in Figure 2, contains a list of seven main titles and their corresponding options.

To navigate the Web-based management interface menu, click a menu title and then click one of its options. When you click an option, the corresponding page opens.

Table 1 lists the main headings in the Web-based management user interface and their associated options.

Table 1 Main headings and options

Main menu titles	**Options**
Summary	Stack Information (stack mode only) Switch Information Switch View Identify Unit Numbers (stack mode only) Stack Numbering (stack mode only)
Configuration	IP System Remote Access SNMPv1 SNMPv3* SNMP Trap MAC Address Table Find MAC Address Port Management High Speed Flow Control Software Download Configuration File Console/Comm Port Stack Operational Mode
Fault	RMON Threshold RMON Event Log System Log
Statistics	Port* Port Error Summary Interface* Ethernet Errors* Transparent Bridging* RMON Ethernet* RMON History*
Application	Port Mirroring Rate Limiting EAPOL Security MAC Address Security* IGMP* VLAN* Spanning Tree* Multilink Trunk* QoS* COPS*
Administration	System Information CPU/Memory Utilization Security* Logout Reset Reset to Defaults

Table 1 Main headings and options

Main menu titles	Options
Support	Help Release Notes Manuals Upgrades
*Has additional menus.	

Tools are provided in the menu to assist you in navigating the Web-based management interface.

Caution: Web browser capabilities such as page bookmarking, refresh, and page forward and page back, function as they would in any other Web site. However, these capabilities do not enhance the functionality of the Web-based management interface. Nortel Networks recommends that you use only the navigation tools provided in the management interface.

Table 2 describes the icons that appear on the menu.

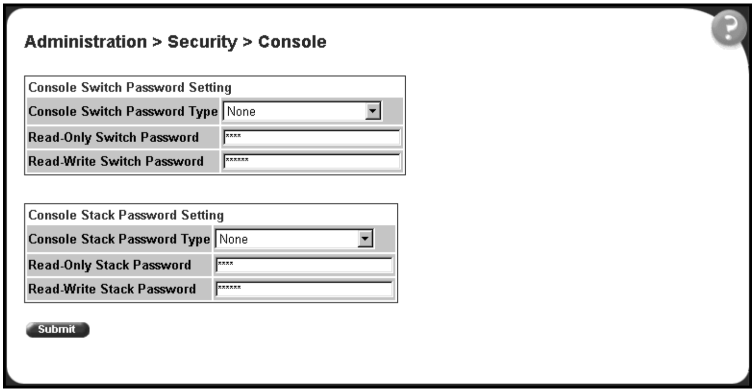
Table 2 Menu icons

Button or icon	Description
➤	This icon identifies a menu title. Click this icon to display its options.
●	This icon identifies a menu title option. Click this icon to display the corresponding page.
◉	This icon identifies a menu title option with a hyperlink to related pages.
〰	This icon is linked an action, for example, logout, reset, or reset to system defaults.
NORTEL NETWORKS	Clicking on the Nortel Networks logo opens the corporate home page in a new Web browser.

Management page

When you click a menu option, the corresponding management page opens. Figure 3 shows the page displayed for the Administration > Security > Console option.

Figure 3 Console page



Administration > Security > Console

Console Switch Password Setting	
Console Switch Password Type	None
Read-Only Switch Password	****
Read-Write Switch Password	******

Console Stack Password Setting	
Console Stack Password Type	None
Read-Only Stack Password	****
Read-Write Stack Password	******

A page is composed of one or more of the following elements:

- Tables and input forms

  The gray cells in a page are display only, and white cells are input fields.

- Check boxes

  You enable or disable a selection by clicking a check box. When a check mark is displayed in the box, that selection is enabled. You disable a selection by clicking the checked box.

- Icons and buttons

  Icons and buttons perform an action concerning the displayed page or the switch. Some pages include a button that opens another page or updates the values shown on the current page. Other pages include icons that initiate an action, such as reformatting the current displayed data as a bar or pie chart.

Table 3 describes the icons that may appear on a pages to assist you in navigation.

Table 3 Page buttons and icons

Icon	Name	Description
📝	Modify	Accesses a modification page for the selected row.
🔍	View	Accesses a view only statistics page for the selected row.
✕	Delete	Deletes a row.
◕	Pie Chart	Displays statistics information in a pie chart format.
📊	Bar Graph	Displays statistics information in a bar graph format.
📈	Line Graph	Displays statistics information in a line graph format.
?	Help	Accesses the Help menu in a new Web browser.
?	Item-Specific Help	Accesses the item-specific Help menu in a new Web browser.
		Note: Text within a table that is highlighted blue and underlined is a hyperlink to a related management page.

Chapter 2
Administering the switch

The administrative options available to you are:

- "Viewing general information," next
- "Configuring system security" on page 44
- "Logging on to the management interface" on page 47
- "Resetting the BPS 2000" on page 49
- "Resetting the BPS 2000 to system defaults" on page 50
- "Logging out of the management interface" on page 51

For more information on the feature discussed in this chapter, refer to *Using the Business Policy Switch 2000 Software Version 2.0*. This book also has instructions using the Console Interface (CI) menus to configure and manage the switch. Refer to *Reference for the Command Line Interface for the Business Policy Switch 2000 Management Software Version 2.0* for instructions on managing the BPS 2000 using the CLI and to *Reference for the Business Policy Switch 2000 Management Software Version 2.0* for instructions on managing the switch using the DM.

Note: To access the software version 2.0 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Viewing general information

You can view an image of the BPS 2000 switch or an image of your entire stack configuration, as information on use of the BPS 2000 CPU and memory capacity.

Viewing system information

You can view an image of the BPS 2000 switch or an image of your entire stack configuration, information about the host device (or stack) and, if provided, the contact person or manager for the switch. The System Information page is also the Web-based management interface home page.

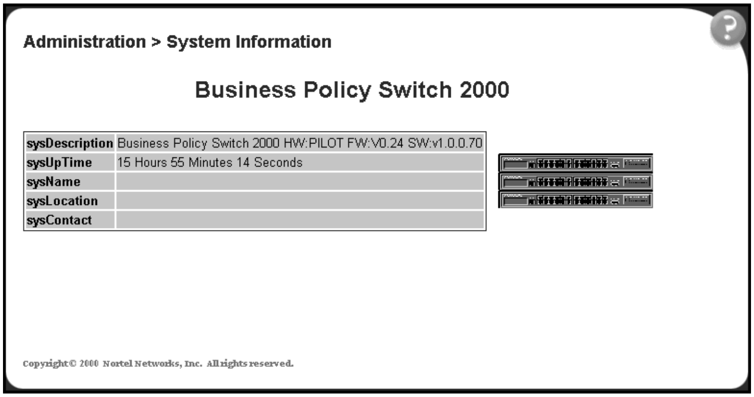
To view system information:

➨ From the main menu, choose Administration > System Information.

The System Information page opens (Figure 4).

Note: You create or modify existing system information parameters on the System page. For more information on configuring system information, refer to Chapter 2.

Figure 4 System Information home page



Administration > System Information

Business Policy Switch 2000

sysDescription	Business Policy Switch 2000 HW:PILOT FW:V0.24 SW:v1.0.0.70
sysUpTime	15 Hours 55 Minutes 14 Seconds
sysName	
sysLocation	
sysContact	

Copyright© 2000 Nortel Networks, Inc. All rights reserved.

Table 4 describes the items on the System Information page.

Table 4 System Information page items

Item	Description
sysDescription	The default description of the Business Policy Switch 2000, including the hardware, firmware, software, and ISVN version numbers.
sysUpTime	The elapsed time since the last network management portion of the system was last re-initialized.
sysName	The name created by the network administrator to identify the switch, for example Finance Group.
sysLocation	The location name created by the network administrator to identify the switch location, for example, first floor.
sysContact	The name and email contact information of the administratively assigned person to contact regarding switch operation.

Viewing CPU and memory utilization

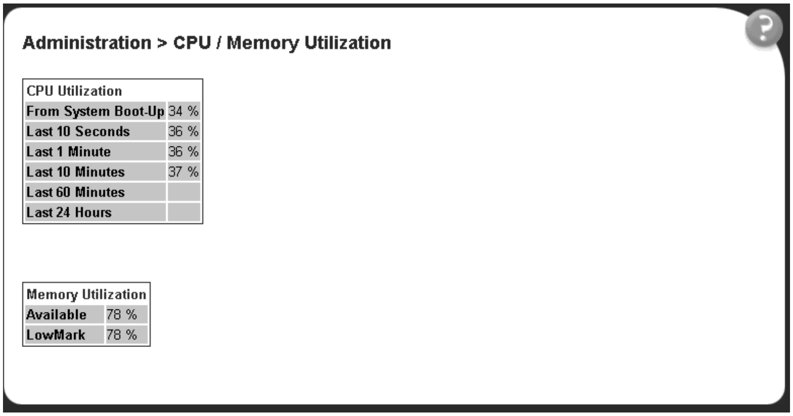
You can view the percentage utilization of the BPS 2000 CPU and memory capacity over time.

To view CPU and memory utilization information:

➨ From the main menu, choose Administration > CPU/Memory Utilization.

The CPU/Memory Utilization page opens (Figure 5).

Figure 5 CPU/Memory Utilization page



Administration > CPU / Memory Utilization

CPU Utilization	
From System Boot-Up	34 %
Last 10 Seconds	36 %
Last 1 Minute	36 %
Last 10 Minutes	37 %
Last 60 Minutes	
Last 24 Hours	

Memory Utilization	
Available	78 %
LowMark	78 %

Table 5 describes the items on the CPU/Memory Utilization page.

Table 5 CPU/Memory Utilization page items

Section	Item	Range	Description
CPU Utilization	From System Boot-Up	1....100	Displays percentage of time system has been busy since boot-up.
	Last 10 Seconds	1..100	Displays percentage of time system has been busy during the last 10 seconds.
	Last 1 Minute	1..100	Displays percentage of time system has been busy during the last 1 minute.
	Last 10 Minutes	1..100	Displays percentage of time system has been busy during the last 10 minutes.
	Last 60 Minutes	1..100	Displays percentage of time system has been busy during the last 60 minutes.
	Last 24 Hours	1..100	Displays percentage of time system has been busy during the last 24 hours.
Memory Utilization	Available	1..100	Displays the percentage of dynamic memory currently available (measured as a percentage of memory available immediately after boot-up).
	LowMark	1..100	Displays the lowest percentage of dynamic memory available since boot-up.

Configuring system security

This section describes the steps you use to build and manage security using the Web-based management interface. For more information on setting security systems, refer to setting EAPOL, MAC security, and IP manager list in Chapter 4.

Setting console, Telnet, and Web passwords

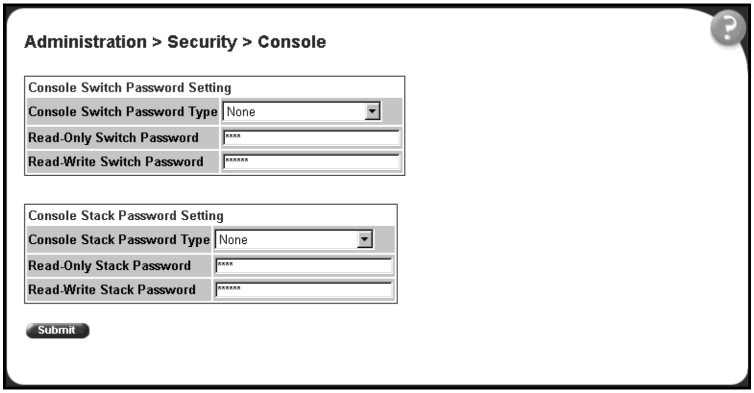
To set console, Telnet, and Web passwords:

1 From the main menu, choose Administration > Security and Console, Telnet, or Web.

The selected password page opens (Figure 6).

Note: The title of the page corresponds to the menu selection you choose. In Figure 6, the network administrator selected Administration > Security > Console.

Figure 6 Console password setting page



Administration > Security > Console

Console Switch Password Setting

Console Switch Password Type	None
Read-Only Switch Password	****
Read-Write Switch Password	******

Console Stack Password Setting

Console Stack Password Type	None
Read-Only Stack Password	****
Read-Write Stack Password	******

Note: Console, Telnet, and Web settings share the same switch and stack password type and password.

Table 6 describes the items on the Console page.

Table 6 Console page items

Section	Item	Setting	Description
Console Switch Password Setting	Console Switch Password Setting Type	(1) None (2) Local Password (3) RADIUS Authentication	Displays the switch password types. Note: The default is None.
	Read-Only Switch Password	1..15 alphanumeric string	Type the read-only password setting for the read-only access user.
	Read-Write Switch Password	1..15 alphanumeric string	Type the read-write password setting for the read-write access user.
Console Stack Password Setting	Console Stack Password Setting Type	(1) None (2) Local Password (3) RADIUS Authentication	Displays the stack password types. Note: The default is None.

Table 6 Console page items

Section	Item	Setting	Description
	Read-Only Stack Password	1..15 alphanumeric string	Type the read-only password setting for the read-only access user.
	Read-Write Stack Password	1..15 alphanumeric string	Type the read-write password setting for the read-write access user.

2 Type the information, or make a selection from the list.

3 Click Submit.

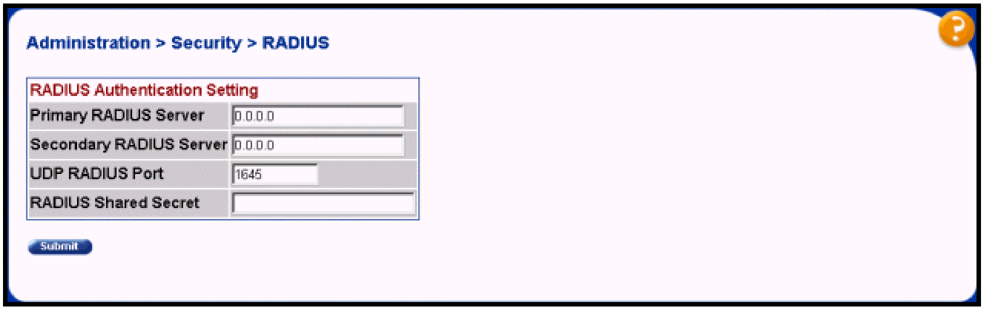
Configuring RADIUS security

To configure RADIUS security parameters:

1 From the main menu, choose Administration > Security > RADIUS.

The RADIUS page opens.

Figure 7 RADIUS page



Administration > Security > RADIUS

RADIUS Authentication Setting

Primary RADIUS Server	0.0.0.0
Secondary RADIUS Server	0.0.0.0
UDP RADIUS Port	1645
RADIUS Shared Secret	

Table 7 describes the items on the RADIUS page.

Table 7 RADIUS page items

Item	Setting	Description
Primary RADIUS Server	XXX.XXX.XXX.XXX	Type a Primary RADIUS server IP address in the appropriate format.
Secondary RADIUS Server	XXX.XXX.XXX.XXX	Type a Secondary RADIUS server IP address in the appropriate format.

Table 7 RADIUS page items

Item	Setting	Description
UDP RADIUS Port	Integer	Type the UDP RADIUS port number.
RADIUS Shared Secret	1..16	Type a unique character string to create a secret password.

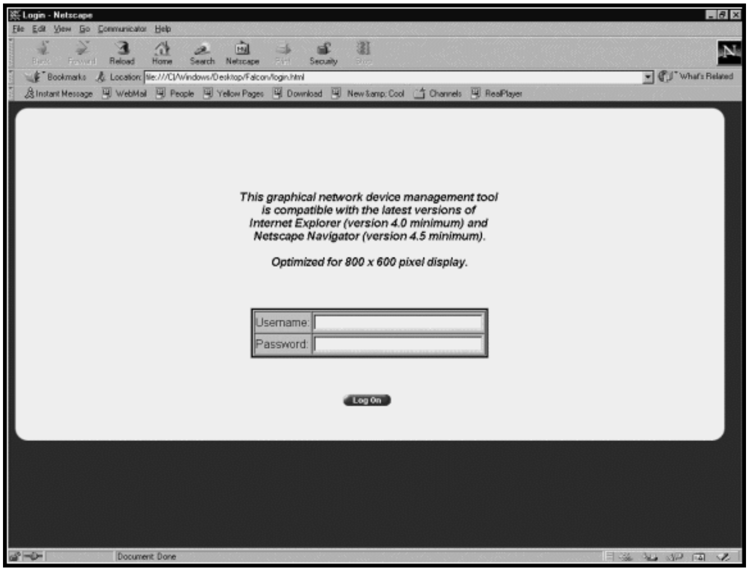
2 Type the information.

3 Click Submit.

Logging on to the management interface

Once switch and stack passwords and RADIUS authentication settings are integrated into the Web-based management user interface, anyone who attempts to use the application is presented with a log on page (Figure 8).

Figure 8 Web-based management interface log on page



This graphical network device management tool is compatible with the latest versions of Internet Explorer (version 4.0 minimum) and Netscape Navigator (version 4.5 minimum).

Optimized for 800 x 600 pixel display.

Login - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Stop
Bookmarks Location: file:///C|/Windows/Desktop/Falcon/login.html
What's Related
Instant Message WebMail People Yellow Pages Download New&amp; Cool Channels RealPlayer
Username:
Password:
Log On
Document: Done

To log on to the Web-based management interface:

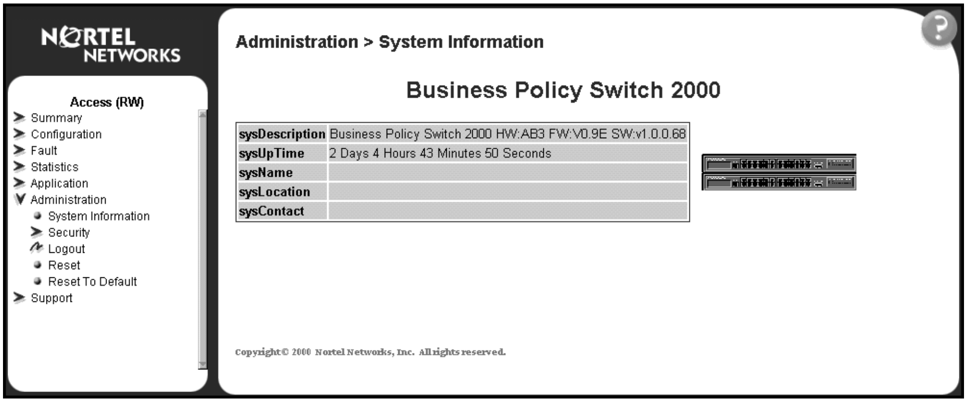
1 In the Username text box, type **`RO`** for read-only access or **`RW`** for read-write access.

2 In the Password text box, type your password.

3 Click Log On.

The System Information home page opens (Figure 9).

Figure 9 System Information home page


NORTEL NETWORKS
Access (RW)
Summary
Configuration
Fault
Statistics
Application
Administration
System Information
Security
Logout
Reset
Reset To Default
Support
?

Administration > System Information

Business Policy Switch 2000

sysDescription	Business Policy Switch 2000 HW:AB3 FW:V0.9E SW:v1.0.0.68
sysUpTime	2 Days 4 Hours 43 Minutes 50 Seconds
sysName	
sysLocation	
sysContact	

Copyright© 2000 Nortel Networks, Inc. All rights reserved.

With Web access enabled, the switch can support up to four concurrent Web page users. Two predefined user levels are available, and each user level has a corresponding username and password.

Table 8 shows an example of the two predefined user levels available and their access level within the Web-based management user interface.

Table 8 User levels and access levels

User level	User name for each level	Password for each user level	Access Level
Read-only	RO	XXXXXXXX	Read only
Read-write	RW	XXXXXXXX	Full read/write access

Resetting the BPS 2000

You can reset a standalone switch, a specific unit in a stack configuration, or an entire stack without erasing any configured switch parameters. While resetting, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress. (Resetting means rebooting in this context.)

To reset the BPS 2000 without making changes (since your last Submit request):

1 From the main menu, choose Administration > Reset.

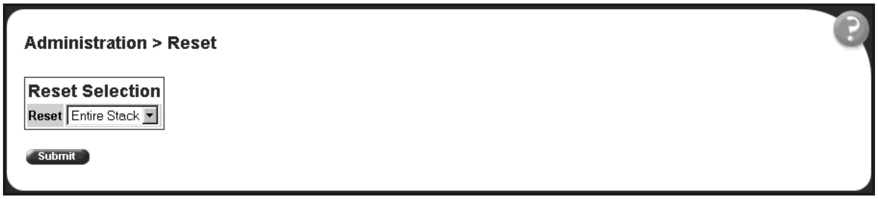
The Reset page opens (Figure 10).

Note: When you are working on a single (nonstacked) switch, the system returns the message:

```
Are you sure you want to reset the switch?
```

When you press OK, the switch resets.

Figure 10 Reset page



Administration > Reset

Reset Selection

Reset: Entire Stack

2 From the list, choose to reset the switch only, or the entire stack.

3 Click Submit.

Note: If you have not configured system password security, a reset returns you to the home page, as shown in Figure 1 on page 35. If you have configured system password security, a reset returns you to a log on page, as shown in Figure 8 on page 47.

Resetting the BPS 2000 to system defaults

You can reset a standalone switch, a specific unit in a stack configuration, or an entire stack, replacing all configured switch parameters with the factory default values.

Caution: If you choose reset to default settings, all configured settings are replaced with factory default settings when you click Submit (Stack Operational Mode is not reset to factory default}. For more information on factory default settings, see *Using the Business Policy Switch 2000 Software Version 2.0*.

During the reset process, the switch initiates a self-test that comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

To reset the BPS 2000 to system defaults:

1 From the main menu, choose Administration > Reset to Default.

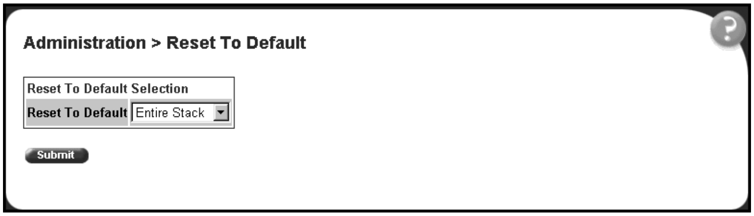
The Reset to Default page opens (Figure 11).

Note: When you are working on a single (nonstacked) switch, the system returns the message:

`Are you sure your want to reset the switch?`

When you press OK, the switch resets.

Figure 11 Reset to Default page



Administration > Reset To Default

Reset To Default Selection

Reset To Default: Entire Stack

2. From the list, choose to reset the switch only to system defaults, or the entire stack.
3. Click Submit.

Note: If you have not configured system password security, a reset returns you to the home page, as shown in Figure 1 on page 35. If you have configured system password security, a reset returns you to a log on page, as shown in Figure 8 on page 47.

Logging out of the management interface

To log out of the Web-based management interface:

1. From the main menu, choose Administration > Logout.

   A message opens prompting you to confirm your request

2. Do one of the following:
   - Click OK to logout of the Web-based management interface.
   - Click Cancel to return to the Web-based management interface home page.

Chapter 3
Viewing summary information

The summary information options are:

- "Viewing stack information," next
- "Viewing summary switch information" on page 55
- "Viewing switch information in real time" on page 57
- "Changing stack numbering" on page 60
- "Identifying unit numbers" on page 62

Note: To access the software version 2.0 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Viewing stack information

You can view a summary of your stack framework, for example, the current version of the running software and the IP address of the Web-based management interface.

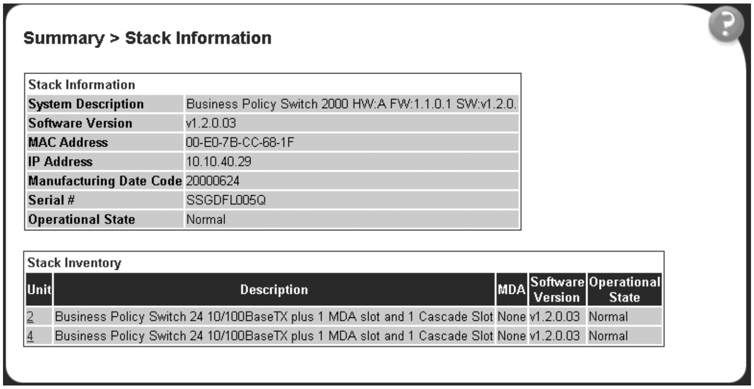
Note: The Web-based management user interface automatically detects the operational mode of your system. If the system is in standalone mode, the Stack Information page is not an option listed in the menu. For information on how to set system operational modes, see "Setting system operational modes" on page 128.

To view stack information:

1 From the main menu, choose Summary > Stack Information.

The Stack Information page opens (Figure 12).

Figure 12 Stack Information page



Summary > Stack Information

Stack Information

System Description	Business Policy Switch 2000 HW:A FW:1.1.0.1 SW:v1.2.0.
Software Version	v1.2.0.03
MAC Address	00-E0-7B-CC-68-1F
IP Address	10.10.40.29
Manufacturing Date Code	20000624
Serial #	SSGDFL005Q
Operational State	Normal

Stack Inventory

Unit	Description	MDA	Software Version	Operational State
2	Business Policy Switch 24 10/100BaseTX plus 1 MDA slot and 1 Cascade Slot	None	v1.2.0.03	Normal
4	Business Policy Switch 24 10/100BaseTX plus 1 MDA slot and 1 Cascade Slot	None	v1.2.0.03	Normal

Table 9 describes the fields on the Stack Information and Stack Inventory sections of the Stack Information page.

Table 9 Stack Information page fields

Section	Fields	Description
Stack Information	System Description	The name created in the configuration process to identify the stack.
	Software Version	The version of the running software.
	MAC Address	The MAC address of the stack.
	IP Address	The IP address of the stack.
	Manufacturing Date Code	The date of manufacture of the board in ASCII format: YYYYMMDD.
	Serial Number	The serial number of the base unit.
	Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured
Stack Inventory	Unit	The unit number assigned to the device by the network manager. For more information on stack numbering, see page 60.
	Description	The description of the device or its subcomponent.
	MDA	The media dependent adapter (MDA) connected to the switch.

Table 9 Stack Information page fields (continued)

Section	Fields	Description
	Software Version	The current running software version.
	Operational State	The current operational state of the stack. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.

2 In the upper-left corner of the Stack Information page, click the number of the device you want to view.

The Stack Information page is updated with information about the selected switch.

Viewing summary switch information

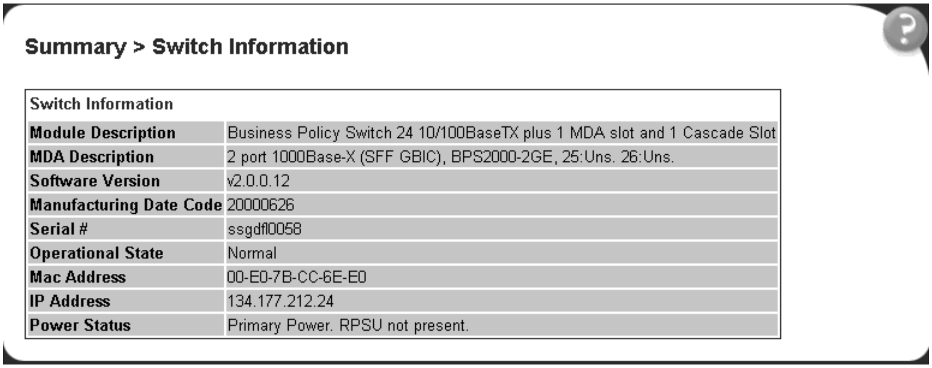
You can view summary information about the switch, for example, the unit number and its corresponding physical description and serial number.

To view summary switch information:

1 From the main menu, choose Summary > Switch Information.

The Switch Information page opens (Figure 13).

Figure 13 Switch Information page



Summary > Switch Information

Switch Information	
Module Description	Business Policy Switch 24 10/100BaseTX plus 1 MDA slot and 1 Cascade Slot
MDA Description	2 port 1000Base-X (SFF GBIC), BPS2000-2GE, 25:Uns. 26:Uns.
Software Version	v2.0.0.12
Manufacturing Date Code	20000626
Serial #	ssgdfl0058
Operational State	Normal
Mac Address	00-E0-7B-CC-6E-E0
IP Address	134.177.212.24
Power Status	Primary Power. RPSU not present.

Table 10 describes the fields on the Switch Information page.

Table 10 Switch Information page fields

Item	Description
Unit	Select the number of the device on which to view summary information. The page is updated with information about the selected switch. For more information on stack numbering, see page 60.
Module Description	The factory set description of the policy switch.
MDA Description	The factory set description of the sub-component/MDA.
Software Version	The version of the running software.
Manufacturing Date Code	The date of manufacture of the board in ASCII format.
Serial Number	The serial number of the policy switch.
Operational State	The current operational state of the device. The operational states are: Other, Not Available, Removed, Disabled, Normal, Reset in Progress, Testing, Warning, Non Fatal Errors, Fatal Error, and Not Configured.
Mac Address	The MAC address of the device.
IP Address	The IP address of the device.
Power Status	The current power status of the device: • Primary Power. RPSU not present • Primary Power. RPSU present • Redundant Power. Primary power failed • Unavailable

2. In the upper-left corner of the Switch Information page, click the number of the device you want to view.

   The Switch Information page is updated with information about the selected switch.

Viewing switch information in real time

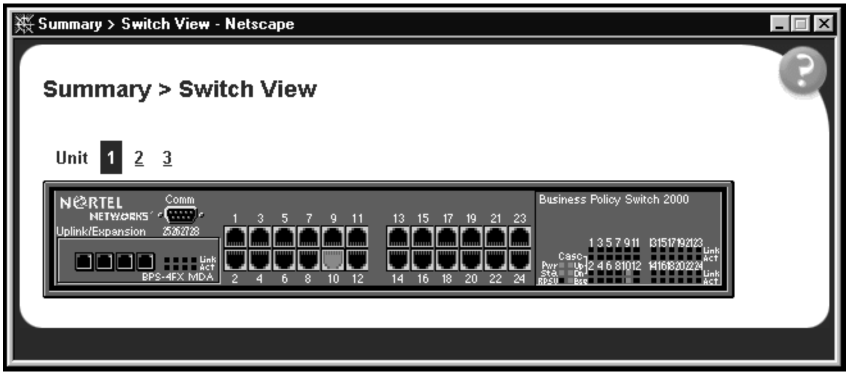
You can display the port and LED status information of a selected policy switch in real time.

To display a physical view of the policy switch:

1 From the main menu, choose Summary > Switch View.

The Switch View page opens in a separate Web browser (Figure 14).

Figure 14 Switch View page


Summary > Switch View - Netscape
Summary > Switch View
Unit 1 2 3
NORTEL NETWORKS
Comm
Uplink/Expansion
Business Policy Switch 2000
BPS-4FX MDA
Link
Act
1 3 5 7 9 11
2 4 6 8 10 12
13 15 17 19 21 23
14 16 18 20 22 24
Pwr
Sta
RPSU
Casc
Up
Dn
Bse

Note: You may be presented with a security warning to click on before the switch view appears.

Table 11 describes the fields on the Switch View page.

Table 11 BPS 2000 switch LED descriptions

Label	Type	Color	State	Meaning
Pwr	Power status	Green	On	DC power is available to the switch's internal circuitry.
			Off	No AC power to switch or power supply failed.
Status	System status	Green	On	Self-test passed successfully and switch is operational.
			Blinking	A nonfatal error occurred during the self-test.
			Off	The switch failed the self-test.
RPSU	RPSU status	Green	On	The switch is connected to the RPSU and can receive power if needed.
			Off	The switch is not connected to the RPSU or RPSU is not supplying power.
CAS Up Stack mode			Off	The switch is in standalone mode.
		Green	On	The switch is connected to the *upstream* unit's Cascade A In connector.
		Amber	On	The Cascade A Out connector (CAS Up) for this switch is looped internally (wrapped to the secondary ring).
CAS Dwn Stack mode			Off	The switch is in standalone mode.
		Green	On	The switch is connected to the *downstream* unit's Cascade A Out connector.
		Amber	On	The Cascade A In connector (CAS Dwn) for this switch is looped internally (wrapped to the secondary ring).

Table 11 BPS 2000 switch LED descriptions (continued)

Label	Type	Color	State	Meaning
Base	Base mode	Green	On	The switch is configured as the stack base unit.
			Off	The switch is *not* configured as the stack base unit (or is in standalone mode).
		Amber	On	This unit is operating as the stack configuration's *temporary base unit*. This condition occurs automatically if the base unit (directly downstream from this unit) fails. If this happens, the following events take place: The two units directly upstream and directly downstream from the failed unit automatically wrap their cascade connectors and indicate this condition by lighting their Cas Up and Cas Dwn LEDs (see Cas Up and Cas Dwn description in this table). If the temporary base unit fails, the next unit directly downstream from this unit becomes the new temporary base unit. This process can continue until there are only two units left in the stack configuration. This automatic failover is a temporary safeguard only. If the stack configuration loses power, the temporary base unit will not power up as the base unit when power is restored. For this reason, you should always assign the temporary base unit as the base unit (set the Unit Select switch to Base) until the failed unit is repaired or replaced.
10/100	10/100 Mb/s port speed indicator	Green	On	The corresponding port is set to operate at 100 Mb/s and the link is good.
		Amber	On	The corresponding port is set to operate at 10 Mb/s and the link is good.
			Off	The link connection is bad or there is no connection to this port.
Link	Link status	Green	On	Valid communications link established.
			Off	The communications link connection is bad or there is no connection to this port.
Activity	Port activity	Green or Amber	Blinking	Indicates network activity for the corresponding port. A high level of network activity can cause the LEDs to appear to be on continuously.

2 In the upper-left corner of the Switch View page, click the number of the device you want to view.

The Switch View page is updated with a view of the selected switch.

Changing stack numbering

If your system is set to “stack” operational mode, you can view existing stack numbering information and renumber the devices in your stack framework. For information on how to set your system’s operational mode, see “Setting system operational modes” on page 128.

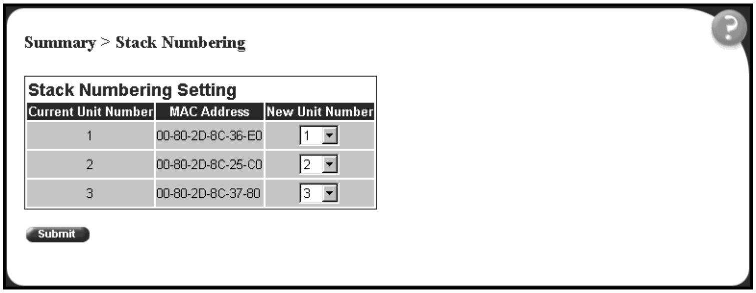
Note: The unit number does not affect the base unit designation.

To view or renumber devices within the stack framework:

1 From the main menu, choose Summary > Stack Numbering.

The Stack Numbering Setting page opens (Figure 15).

Figure 15 Stack Numbering Setting page



Summary > Stack Numbering

Stack Numbering Setting

Current Unit Number	MAC Address	New Unit Number
1	00-80-2D-8C-36-E0	1
2	00-80-2D-8C-25-C0	2
3	00-80-2D-8C-37-80	3

Table 12 describes the fields on the Stack Numbering Setting page.

Table 12 Stack Numbering Setting page fields

Item	Range	Description
Current Unit Number	1..8	Unit number previously assigned to the policy switch. The entries in this column are displayed in order of their current physical cabling with respect to the base unit, and can show nonconsecutive unit numbering if one or more units were previously moved or modified. The entries can also include unit numbers of units that are no longer participating in the stack (not currently active).

Table 12 Stack Numbering Setting page fields (continued)

Item	Range	Description
MAC Address	XX.XX.XX.XX.XX.XX	MAC address of the corresponding unit listed in the Current Unit Number field.
New Unit Number	1..8, None	Choose a new number to assign to your selected policy switch. Note: If you leave the field blank, the system automatically selects the next available number.

2 Choose the new number to assign to your switch.

3 Click Submit.

A message opens prompting you to confirm your request.

4 Do one of the following:

- Click OK to renumber the stack.
- Click Cancel to return to the Stack Numbering page without making changes.

Identifying unit numbers

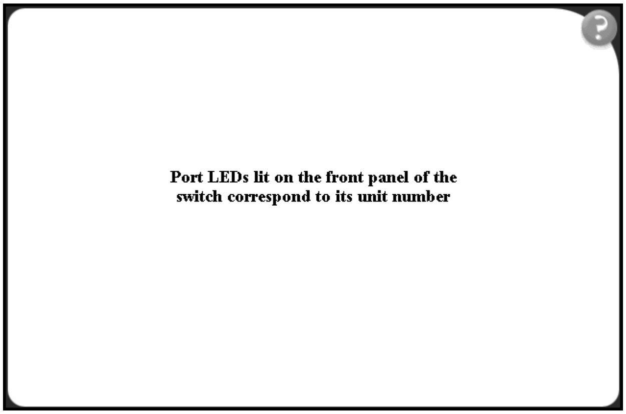
You can identify the unit numbers of the switches participating in a stack configuration by viewing the LEDs on the front panel of each switch.

To identify unit numbers in your configuration:

1. From the main menu, choose Summary > Identify Unit Numbers.

   The Identify Unit Numbers page opens (Figure 16).

Figure 16 Identify Unit Numbers page



Port LEDs lit on the front panel of the switch correspond to its unit number

2. To continue viewing summary information or to start the configuration process, choose another option from the main menu.

Chapter 4
Configuring the switch

The switch configuration options available to you are:

- "Configuring BootP, IP, and gateway settings," (next)
- "Modifying system settings" on page 67
- "About SNMP" on page 68
- "Configuring SNMPv1" on page 69
- "Configuring SNMPv3" on page 70
- "Configuring SNMP traps" on page 89
- "Configuring EAPOL-based security" on page 91
- "Managing remote access by IP address" on page 94
- "Configuring MAC address-based security" on page 96
- "Viewing learned MAC addresses by VLAN" on page 108
- "Locating a specific MAC address" on page 109
- "Configuring port's autonegotiation, speed, duplex, status, and alias" on page 111
- "Configuring high speed flow control" on page 114
- "Downloading switch images" on page 116
- "Storing and retrieving a switch configuration file from a TFTP server" on page 124
- "Configuring port communication speed" on page 127
- "Setting system operational modes" on page 128

Note: To access the software version 2.0 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Configuring BootP, IP, and gateway settings

You can configure your BootP mode settings, create and modify your in-band stack and in-band switch IP addresses and in-band subnet mask parameters, and configure the IP address of your default gateway. Beginning with software version 2.0, you can configure IP addresses for individual units in a stack.

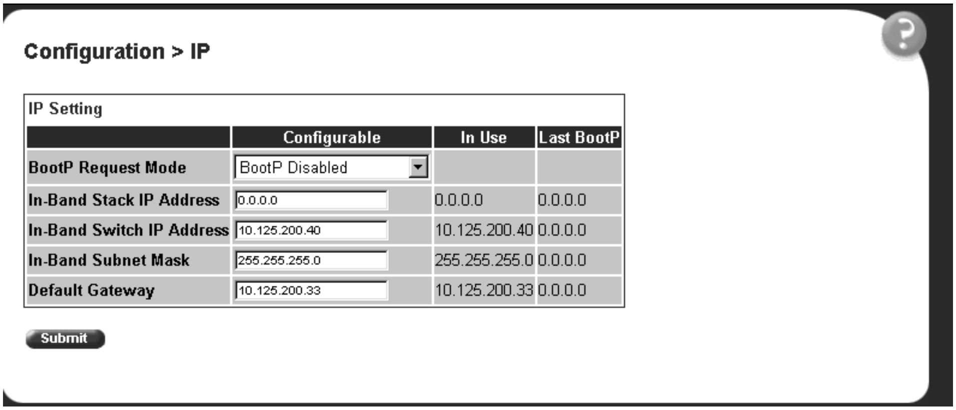
Note: Settings take effect immediately when you click Submit.

To configure BootP, IP, and gateway settings:

1 From the main menu, choose Configuration > IP.

The IP page opens (Figure 17).

Figure 17 IP page for a standalone BPS 2000

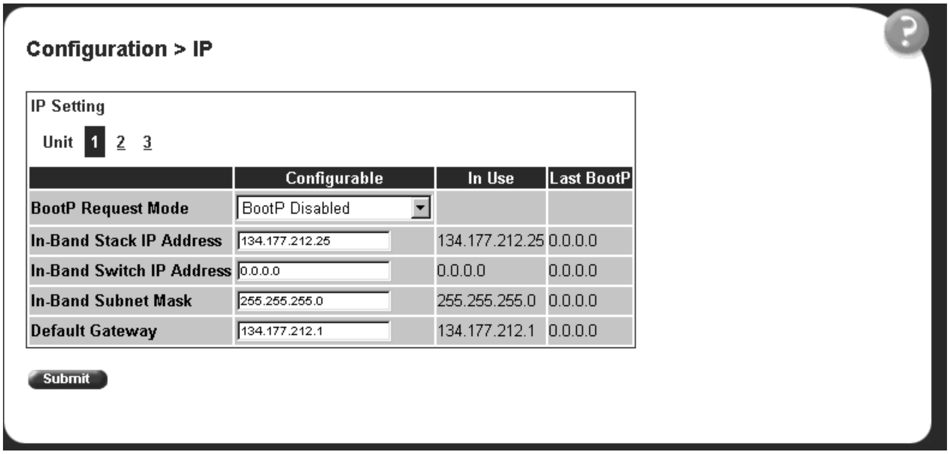


Configuration > IP

IP Setting

	Configurable	In Use	Last BootP
BootP Request Mode	BootP Disabled		
In-Band Stack IP Address	0.0.0.0	0.0.0.0	0.0.0.0
In-Band Switch IP Address	10.125.200.40	10.125.200.40	0.0.0.0
In-Band Subnet Mask	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	10.125.200.33	10.125.200.33	0.0.0.0

Figure 18 IP page for a stack



Configuration > IP

IP Setting

Unit **1** 2 3

	Configurable	In Use	Last BootP
BootP Request Mode	BootP Disabled		
In-Band Stack IP Address	134.177.212.25	134.177.212.25	0.0.0.0
In-Band Switch IP Address	0.0.0.0	0.0.0.0	0.0.0.0
In-Band Subnet Mask	255.255.255.0	255.255.255.0	0.0.0.0
Default Gateway	134.177.212.1	134.177.212.1	0.0.0.0

Note: To change the IP information for a specific unit in the stack, choose that unit and enter the desired IP information into the In-Band Switch IP address field.

Table 13 describes the items on the IP page.

Table 13 IP page items

Section	Item	Range	Description
Boot Mode Setting	BootP Request Mode	BootP When Needed	Choose this mode to inform the switch to send a BootP request when the switch IP address stored in nonvolatile memory is the factory default value. If the stored IP address differs from the factory default value, the switch uses the stored network parameters. If the switch cannot find a BootP server, it tries five more times to find one and then defaults to the factory settings
		BootP Always	Choose this mode to inform the switch, each time the switch boots, to ignore any stored network parameters and send a BootP request. If the BootP request fails, the switch boots with the factory default IP configuration. This setting disables remote management if no BootP server is set up for the switch, but it allows the switch to boot normally.
		BootP Disabled	Choose this mode to inform the switch, each time the switch boots, to use the IP configuration parameters stored in non-volatile memory. If a BootP configuration is in progress when you issue this command, the BootP configuration stops.

Table 13 IP page items

Section	Item	Range	Description
		BootP or Last Address	Choose this mode to inform the switch, at each startup, to obtain its IP configuration using BootP. If the BootP request fails, the switch uses the network parameters stored in its non-volatile memory. Note: Valid parameters obtained in using BootP always replace current information stored in the non-volatile memory.
		Note: Whenever the switch is broadcasting BootP requests, the BootP process times out if a reply is not received within (approximately) 7 minutes. When the process times out, the BootP request mode automatically changes to BootP Disabled mode. To restart the BootP process, change the BootP request mode to any of the three following modes: BootP When Needed, BootP Always, or to BootP or Last Address.	
IP Setting	In-Band Stack IP Address	XXX.XXX.XXX.XXX	Type a new stack IP address in the appropriate format.
	In-Band Switch IP Address	XXX.XXX.XXX.XXX	Type a new switch IP address in the appropriate format. Note: When the IP address is entered in the In-Band IP Address field, and the In-Band Subnet Mask field value is not present, the software provides an *in-use* default value for the In-Band Subnet Mask field that is based on the class of the IP address entered in the In-Band IP Address field.
	In-Band Subnet Mast	XXX.XXX.XXX.XXX	Type a new subnet mask in the appropriate format.
	In-Use		The column header for the read-only fields in this screen. The data displayed in this column represents data that is currently in use.
	Last BootP		The column header for the read-only fields in this screen. The read-only data displayed in this column represents data obtained from the last BootP reply received.
Gateway Setting	Default Gateway	XXX.XXX.XXX.XXX	Type an IP address for the default gateway in the appropriate format.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Modifying system settings

You can create or modify the system name, system location, and network manager contact information.

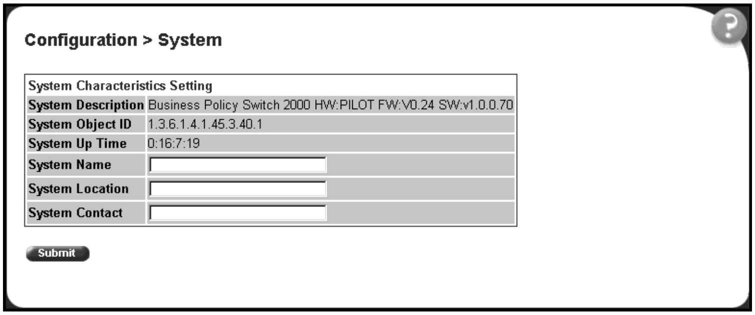
Note: The configurable parameters on the System page are displayed in a read only-format on the Web-based management user interface System Information home page (see Figure 1 on page 35).

To configure system settings:

1 From the main menu, choose Configuration > System.

The System page opens (Figure 19).

Figure 19 System page



Configuration > System

System Characteristics Setting

System Description	Business Policy Switch 2000 HW:PILOT FW:V0.24 SW:v1.0.0.70
System Object ID	1.3.6.1.4.1.45.3.40.1
System Up Time	0:16:7:19
System Name	
System Location	
System Contact	

Table 14 describes the items on the System page.

Table 14 System page items

Item	Range	Description
System Description		The factory set description of the hardware and software versions.
System Object ID		The character string that the vendor created to uniquely identify this device.
System Up Time		The elapsed time since the last network management portion of the system was last re-initialized. Note: This field is updated only when the screen is redisplayed.
System Name	0..255	Type a character string to create a name to identify the switch, for example Finance Group.
System Location	0..255	Type a character string to create a name for the switch location, for example, First Floor.
System Contact	0..255	Type a character string to create the contact information for the network manager or the selected person to contact regarding switch operation, for example, mcarlson@company.com Note: To operate correctly with the Web interface, the system contact should be an e-mail address.

2. Type information in the text boxes.
3. Click Submit.

About SNMP

Simple Network Management Protocol (SNMP) is the standard for network management that uses a common software agent to manage local and wide area network equipment from different vendors; part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite and defined in RFC1157. SNMPv1 is version one, or the original standard protocol. SNMPv3 is a combination of proposal updates to SNMP, most of which deal with security.

Configuring SNMPv1

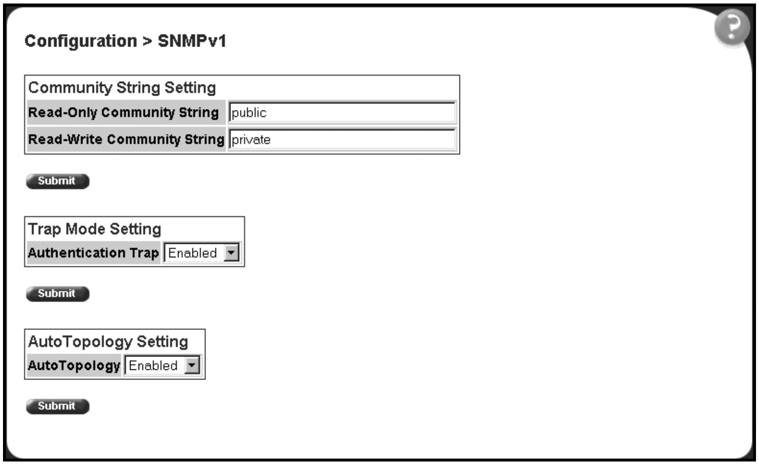
You can configure SNMPv1 read-write and read-only community strings, enable or disable trap mode settings, and/or enable or disable the Autotopology feature. The Autotopology feature, when enabled, performs a process that recognizes any device on the managed network and defines and maps its relation to other network devices in real time.

To configure the community string, trap mode, and Autotopology settings and features:

1 From the main menu, choose Configuration > SNMPv1.

The SNMPv1 page opens (Figure 20).

Figure 20 SNMPv1 page



Configuration > SNMPv1

Community String Setting

Read-Only Community String	public
Read-Write Community String	private

Trap Mode Setting

Authentication Trap	Enabled

AutoTopology Setting

AutoTopology	Enabled

Table 15 describes the items on the SNMPv1 page.

Table 15 SNMPv1 page items

Section	Item	Range	Description
Community String Setting	Read-Only Community String	1..32	Type a character string to identify the community string for the SNMPv1 read-only community, for example, public or private. The default value is public.
	Read-Write Community String	1..32	Type a character string to identify the community string for the SNMPv1 read-write community, for example, public or private. The default value is private.
Trap Mode Setting	Authentication Trap	(1) Enable (2) Disable	Choose to enable or disable the authentication trap.
AutoTopology Setting	AutoTopology	(1) Enable (2) Disable	Choose to enable or disable the autotopology feature.

2 Type information in the text boxes, or select from a list.

3 Click Submit in any section to save your changes.

Configuring SNMPv3

This section describes the steps to build and manage SNMPv3 in the Web-based management user interface.

Viewing SNMPv3 system information

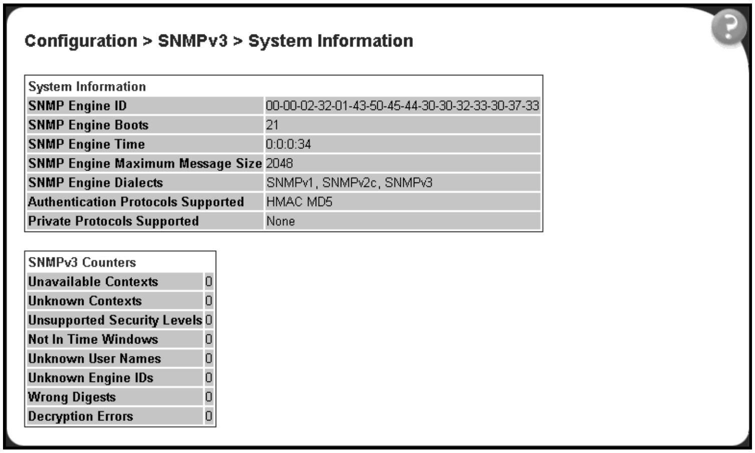
You can view information about the SNMPv3 engine that exists and the private protocols that are supported in your network configuration. You can also view information about packets received by the system having particular errors, such as unavailable contexts, unknown contexts, decrypting errors, or unknown user names.

To view SNMPv3 system information:

1 From the main menu, choose Configuration > SNMPv3 > System Information.

The System Information page opens (Figure 21).

Figure 21 System Information page



Configuration > SNMPv3 > System Information

System Information	
SNMP Engine ID	00-00-02-32-01-43-50-45-44-30-30-32-33-30-37-33
SNMP Engine Boots	21
SNMP Engine Time	0:0:0:34
SNMP Engine Maximum Message Size	2048
SNMP Engine Dialects	SNMPv1 , SNMPv2c , SNMPv3
Authentication Protocols Supported	HMAC MD5
Private Protocols Supported	None

SNMPv3 Counters	
Unavailable Contexts	0
Unknown Contexts	0
Unsupported Security Levels	0
Not In Time Windows	0
Unknown User Names	0
Unknown Engine IDs	0
Wrong Digests	0
Decryption Errors	0

Table 16 describes the fields on the System Information section of the SNMPv3 System Information page.

Table 16 System Information section fields

Item	**Description**
SNMP Engine ID	The SNMP engine's identification number.
SNMP Engine Boots	The number of times that the SNMP engine has re-initialized itself since its initial configuration.
SNMP Engine Time	The number of seconds since the SNMP engine last incremented the snmpEngineBoots object.
SNMP Engine Maximum Message Size	The maximum length, in octets, of an SNMP message which this SNMP engine can send or receive and process determined as the minimum of the maximum message size values supported among all transports available to and supported by the engine.
SNMP Engine Dialects	The SNMP dialect the engine recognizes. The dialects are:SNMP1v1, SNMPv2C, and SNMPv3.
Authentication Protocols Supported	The registration point for standards-track authentication protocols used in SNMP Management Frameworks. The registration points are: None, HMAC MD5. Note: The Business Policy Switch 2000 supports only the MD5 authentication protocol.
Private Protocols Supported	The registration point for standards-track privacy protocols used in SNMP Management Frameworks. The registration points are: None or CBC-DES. Note: The Business Policy Switch 2000 does not support privacy protocols.

Table 17 describes the fields on the SNMPv3 Counters section of the SNMPv3 System Information page.

Table 17 SNMPv3 Counters section fields

Item	Description
Unavailable Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unavailable.
Unknown Contexts	The total number of packets dropped by the SNMP engine because the context contained in the message was unknown.
Unsupported Security Levels	The total number of packets dropped by the SNMP engine because they requested a security level that was unknown to the SNMP engine or otherwise unavailable.
Not in Time Windows	The total number of packets dropped by the SNMP engine because they appeared outside of the authoritative SNMP engine's window.
Unknown User Names	The total number of packets dropped by the SNMP engine because they referenced an unknown user.
Unknown Engine IDs	The total number of packets dropped by the SNMP engine because they referenced an snmpEngineID that was not known to the SNMP engine.
Wrong Digests	The total number of packets dropped by the SNMP engine because they did not contain the expected digest value.
Decryption Errors	The total number of packets dropped by the SNMP engine because they could not be decrypted.

Configuring user access to SNMPv3

You can view a table of all current SNMPv3 user security information such as authentication/privacy protocols in use, and create or delete SNMPv3 system user configurations.

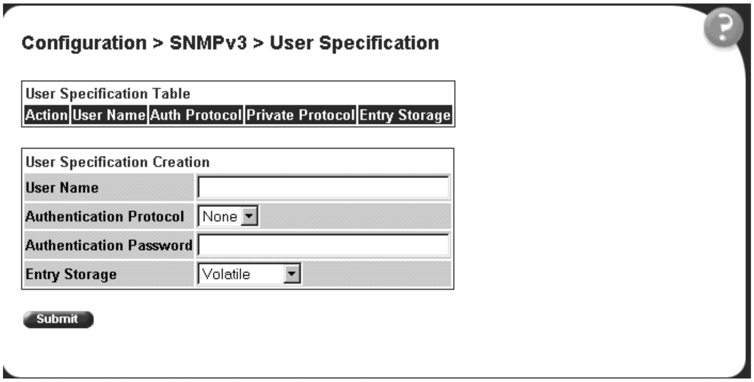
Creating an SNMPv3 system user configuration

To create an SNMPv3 system user configuration:

1. From the main menu choose Configuration > SNMPv3 > User Specification.

   The User Specification page opens (Figure 22).

Figure 22 User Specification page



Configuration > SNMPv3 > User Specification

User Specification Table

Action	User Name	Auth Protocol	Private Protocol	Entry Storage

User Specification Creation

User Name	
Authentication Protocol	None
Authentication Password	
Entry Storage	Volatile

Table 18 describes the items on the User Specification Table section of the User Specification page.

Table 18 User Specification Table section items

Item and MIB association	**Description**
☒	Deletes the row.
User Name (usmUserSecurityName)	The name of an existing SNMPv3 user.
Authentication Protocol (usmUserAuthProtocol)	Indicates whether the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated by the MD5 authentication protocol. Note: The Business Policy Switch 2000 supports only the MD5 authentication protocol.
Private Protocol (usmUserPrivProtocol)	Displays whether or not messages sent on behalf of this user to or from the SNMP engine identified by usmUserEngineID can be protected from disclosure, and if so, the type of privacy protocol which is used.
Entry Storage	The current storage type for this row. If “Volatile” is displayed, information is dropped (lost) when you turn the power off. If non-volatile is displayed, information is saved in NVRAM when you turn the power off

Table 19 describes the items on the User Specification Creation section of the User Specification page.

Table 19 User Specification Creation section items

Item and MIB association	**Range**	**Description**
User Name	1..32	Type a string of characters to create an identity for the user.
Authentication Protocol (usmUserAuthProtocol)	None MD5	Choose whether or not the message sent on behalf of this user to/from the SNMP engine identified UserEngineID can be authenticated with the MD5 protocol. Note: The Business Policy Switch 2000 supports only the MD5 authentication protocol.
Authentication Password (usmUserAuthPassword)	1..32	Type a string of character to create a password to use in conjunction with the authorization protocol.
Entry Storage (usmUserStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the User Specification Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new configuration is displayed in the User Specification Table (Figure 22).

Deleting an SNMPv3 system user configuration

To delete an existing SNMPv3 user configuration:

1. From the main menu, choose Configuration > SNMPv3 > User Specification.

   The User Specification page opens (Figure 22).

2. In the User Specification Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the SNMPv3 user configuration.
   - Click Cancel to return to the User Specification page without making changes.

Configuring an SNMPv3 system user group membership

You can view a table of existing SNMPv3 group membership configurations and map or delete an SNMPv3 user to group configuration.

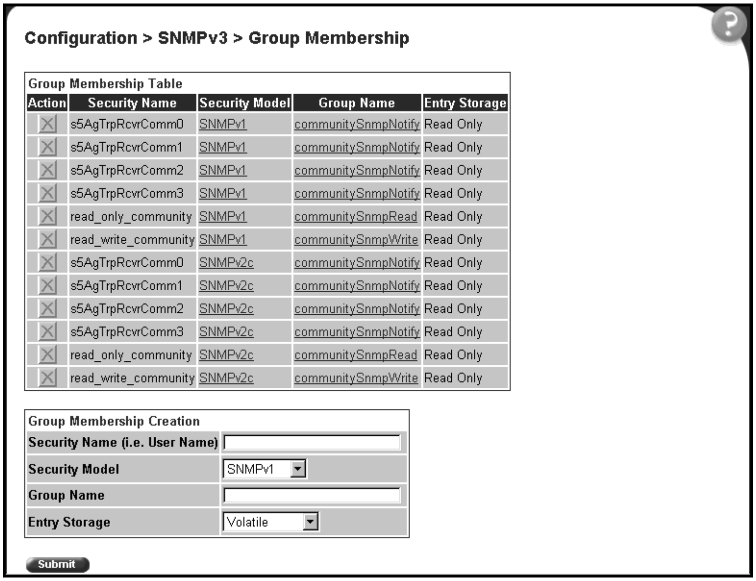
Mapping an SNMPv3 system user to a group

To map an SNMPv3 system user to a group:

1. From the main menu, choose Configuration > SNMPv3 > Group Membership.

   The Group Membership page opens (Figure 23).

Figure 23 Group Membership page



Configuration > SNMPv3 > Group Membership

Group Membership Table

Action	Security Name	Security Model	Group Name	Entry Storage
☒	s5AgTrpRcvrComm0	SNMPv1	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm1	SNMPv1	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm2	SNMPv1	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm3	SNMPv1	communitySnmpNotify	Read Only
☒	read_only_community	SNMPv1	communitySnmpRead	Read Only
☒	read_write_community	SNMPv1	communitySnmpWrite	Read Only
☒	s5AgTrpRcvrComm0	SNMPv2c	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm1	SNMPv2c	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm2	SNMPv2c	communitySnmpNotify	Read Only
☒	s5AgTrpRcvrComm3	SNMPv2c	communitySnmpNotify	Read Only
☒	read_only_community	SNMPv2c	communitySnmpRead	Read Only
☒	read_write_community	SNMPv2c	communitySnmpWrite	Read Only

Group Membership Creation

Security Name (i.e. User Name)	
Security Model	SNMPv1
Group Name	
Entry Storage	Volatile

Table 20 describes the items on the Group Membership page.

Table 20 Group Membership page items

Item and MIB association	Range	Description
☒		Deletes the row.
Security Name (vacmSecurityToGroupStatus)	1..32	Type a string of character to create a security name for the principal which is mapped by this entry to a group name.
Security Model (vacmSecurityToGroupStatus)	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model within which the security name to group name mapping is valid.
Group Name (vacmGroupName)	1..32	Type a string of character to specify the group name.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Group Membership Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Group Membership Table.

Deleting an SNMPv3 group membership configuration

To delete an SNMPv3 group membership configuration:

1 From the main menu, choose Configuration > SNMPv3 > Group Membership.

The Group Membership page opens (Figure 23).

2 In the Group Membership Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the group membership configuration.
- Click Cancel to return to the Group Membership page without making changes.

➡ **Note:** This Group Membership Table section of the Group Membership page contains hyperlinks to the SNMPv3 User Specification and Group Access Rights pages. For more information on these pages, see "Configuring user access to SNMPv3" on page 72 and "Configuring SNMPv3 group access rights" on page 78.

Configuring SNMPv3 group access rights

You can view a table of existing SNMPv3 group access rights configurations, and you can create or delete a group's SNMPv3 system-level access rights.

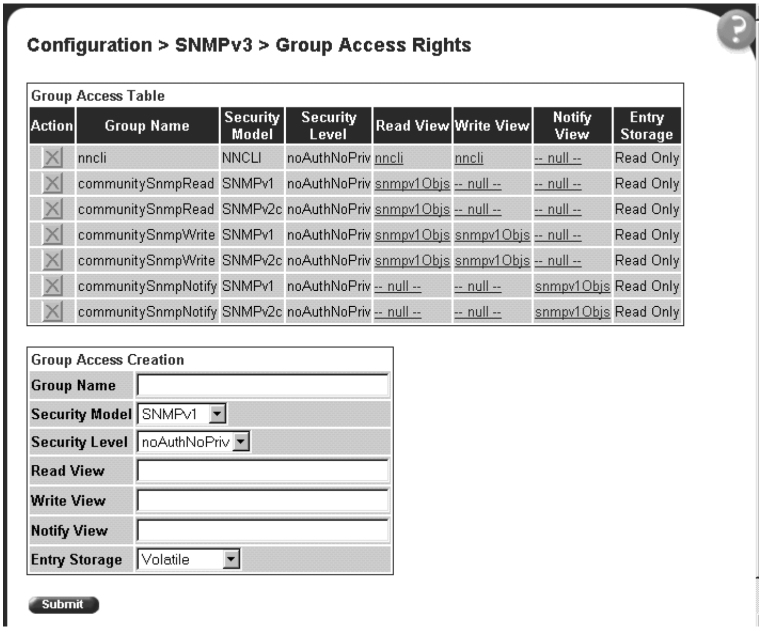
Creating an SNMPv3 group access rights configuration

To create a group's SNMPv3 system-level access right configuration:

1. From the main menu, choose Configuration > SNMPv3 > Group Access Rights.

   The Group Access Rights page opens (Figure 24).

Figure 24 Group Access Rights page



Configuration > SNMPv3 > Group Access Rights

Group Access Table

Action	Group Name	Security Model	Security Level	Read View	Write View	Notify View	Entry Storage
☒	nncli	NNCLI	noAuthNoPriv	nncli	nncli	-- null --	Read Only
☒	communitySnmpRead	SNMPv1	noAuthNoPriv	snmpv1Objs	-- null --	-- null --	Read Only
☒	communitySnmpRead	SNMPv2c	noAuthNoPriv	snmpv1Objs	-- null --	-- null --	Read Only
☒	communitySnmpWrite	SNMPv1	noAuthNoPriv	snmpv1Objs	snmpv1Objs	-- null --	Read Only
☒	communitySnmpWrite	SNMPv2c	noAuthNoPriv	snmpv1Objs	snmpv1Objs	-- null --	Read Only
☒	communitySnmpNotify	SNMPv1	noAuthNoPriv	-- null --	-- null --	snmpv1Objs	Read Only
☒	communitySnmpNotify	SNMPv2c	noAuthNoPriv	-- null --	-- null --	snmpv1Objs	Read Only

Group Access Creation

Group Name	
Security Model	SNMPv1
Security Level	noAuthNoPriv
Read View	
Write View	
Notify View	
Entry Storage	Volatile

Table 21 describes the items on the Group Access Rights page.

Table 21 Group Access Rights page items

Item and MIB association	Range	Description
☒		Deletes the row.
Group Name (vacmAccessToGroupStatus)	1..32	Type a character string to specify the group name to which access is granted.
Security Model (vacmAccessSecurityModel)l	(1) SNMPv1 (2) SNMPv2c (3) USM	Choose the security model to which access is granted.
Security Level (vacmAccessSecurityLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the minimum level of security required in order to gain the access rights allowed to the group.
Read View (vacmAccessReadViewName)	1..32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes read access.
Write View (vacmAccessWriteViewName)	1..32	Type a character string to identify the MIB view of the SNMP context to which this entry authorizes write access.
Notify View (vacmAccessNotifyViewName)	1..32	Type a character string to identify the MIB view to which this entry authorizes access to notifications.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2. In the Group Access Creation section, type information in the text boxes, or select from a list.
3. Click Submit.

   The new entry appears in the Group Access Table.

Deleting an SNMPv3 group access rights configuration

To delete a n SNMPv3 group access configuration:

1. From the main menu, choose Configuration > SNMPv3 > Group Access Rights.

   The Group Access Rights page opens (Figure 24).

2 In the Group Access Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the group access configuration.
- Click Cancel to return to the Group Access Rights page without making changes.

➡ **Note:** This Group Access Table section of the Group Access Rights page contains hyperlinks to the Management Information View page. For more information, see "Configuring an SNMPv3 management information view" on page 80.

Configuring an SNMPv3 management information view

You can view a table of existing SNMPv3 management information view configurations, and you can create or delete SNMPv3 management information view configurations.

➡ **Note:** A view may consist of multiple entries in the table, each with the same view name, but a different view subtree.

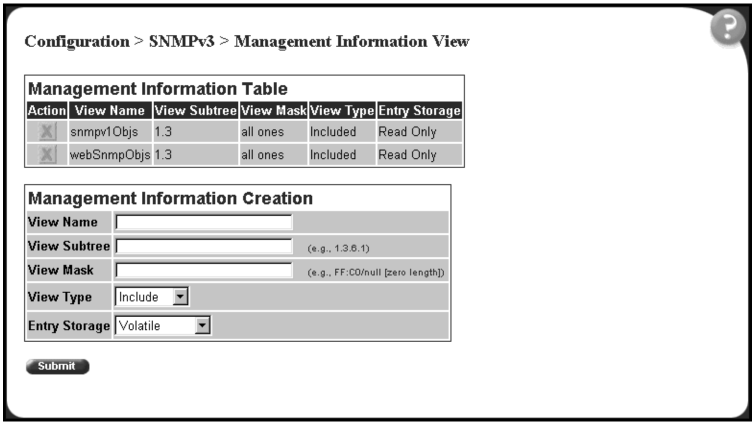
Creating an SNMPv3 management information view configuration

To create an SNMPv3 management information view configuration:

1 From the main menu, choose Configuration > SNMPv3 > Management Info View.

The Management Information page opens (Figure 25).

Figure 25 Management Information View page



Configuration > SNMPv3 > Management Information View

Management Information Table

Action	View Name	View Subtree	View Mask	View Type	Entry Storage
☒	snmpv1Objs	1.3	all ones	Included	Read Only
☒	webSnmpObjs	1.3	all ones	Included	Read Only

Management Information Creation

View Name		
View Subtree		(e.g., 1.3.6.1)
View Mask		(e.g., FF:C0/null [zero length])
View Type	Include	
Entry Storage	Volatile	

Table 22 describes the items on the Management Information View page.

Table 22 Management Information View page items

Item and MIB association	Range	Description
☒		Deletes the row.
View Name (vacmViewTreeFamilyViewName)	1..32	Type a character string to create a name for a family of view subtrees.
View Subtree (vacmViewTreeFamilySubtree)	X.X.X.X.X...	Type an object identifier (OID) to specify the MIB subtree which, when combined with the corresponding instance of vacmViewTreeFamilyMask, defines a family of view subtrees. Note: If no OID is entered and the field is blank, a default mask value consisting of "1s" is recognized.
View Mask (vacmViewTreeFamilyMask)	Octet String (0..16)	Type the bit mask which, in combination with the corresponding instance of vacmViewFamilySubtree, defines a family of view subtrees.
View Type (vacmViewTreeFamilyType)	(1) Included (2) Excluded	Choose to include or exclude a family of view subtrees.
Entry Storage (vacmSecurityToGroupStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2. In the Management Information Creation section, type information in the text boxes, or select from a list.
3. Click Submit.

   The new entry appears in the Management Information Table (Figure 25).

Deleting an SNMPv3 management information view configuration

To delete an existing SNMPv3 management information view configuration:

1. From the main menu, choose Configuration > SNMPv3 > Management Info View.

   The Management Information page opens (Figure 25).

2. In the Management Information Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the management information view configuration.
   - Click Cancel to return to the table without making changes.

Configuring an SNMPv3 system notification entry

You can view a table of existing SNMPv3 system notification configurations, and you can configure specific SNMPv3 system notification types with particular message recipients and delete SNMPv3 notification configurations.

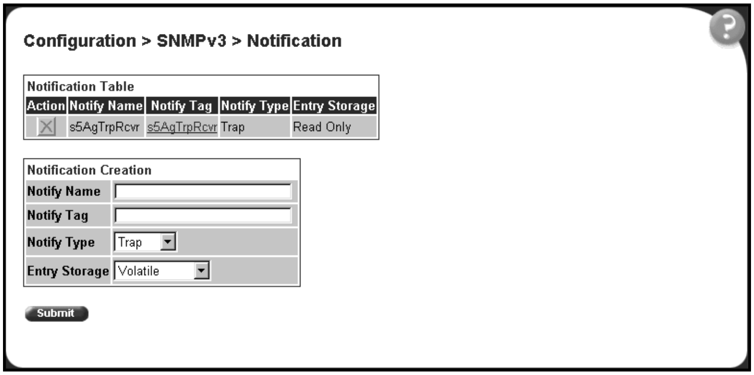
Creating an SNMPv3 system notification configuration

To create an SNMPv3 system notification configuration:

1 From the main menu, choose Configuration > SNMPv3 > Notification.

The Notification page opens (Figure 26).

Figure 26 Notification page



Configuration > SNMPv3 > Notification

Notification Table

Action	Notify Name	Notify Tag	Notify Type	Entry Storage
☒	s5AgTrpRcvr	s5AgTrpRcvr	Trap	Read Only

Notification Creation

Notify Name	
Notify Tag	
Notify Type	Trap
Entry Storage	Volatile

Table 23 describes the items on the Notification page.

Table 23 Notification page items

Item and MIB association	Range	Description
☒		Deletes the row.
Notify Name (snmpNotifyRowStatus)	1..32	Type a character string to identify the entry.
Notify Tag (snmpNotifyTag)	1..32	Type a value which to use to select entries in the snmpTargetAddrTable. Any entry in the snmpTargetAddrTable which contains a tag value which is equal to the value of an instance of this object is selected. If this object carries a zero length, no entries are selected
Notify Type (snmpNotifyType)	(1) Trap (2) Inform	Choose the type of notification to generate.
Entry Storage (snmpNotifyStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Notification Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Notification Table (Figure 26).

➡ **Note:** This Notification Table section of the Notification page contains hyperlinks to the Target Parameter page. For more information, see "Configuring an SNMPv3 management target parameter" on page 87.

Deleting an SNMPv3 system notification configuration

To delete an SNMPv3 notification configuration:

1 From the main menu, choose Configuration > SNMPv3 > Notification.

The Notification page opens (Figure 26).

2 In the Notification Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the notification configuration.
- Click Cancel to return to the table without making changes.

Configuring an SNMPv3 management target address

You can view a table of existing SNMPv3 management target configurations, create SNMPv3 management target address configurations that associate notifications with particular recipients and delete SNMPv3 target address configurations.

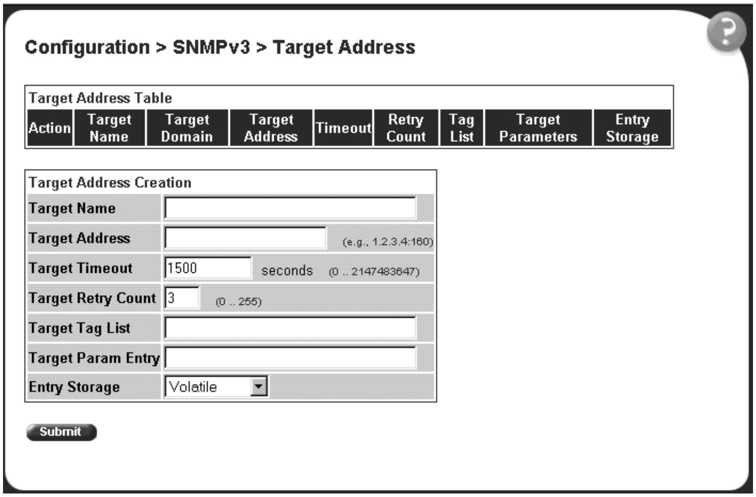
Creating an SNMPv3 target address configuration

To create an SNMPv3 target address configuration:

1 From the main menu, choose Configuration > SNMPv3 > Target Address.

The Target Address page opens (Figure 27).

Figure 27 Target Address page



Configuration > SNMPv3 > Target Address

Target Address Table

Action	Target Name	Target Domain	Target Address	Timeout	Retry Count	Tag List	Target Parameters	Entry Storage

Target Address Creation

Target Name	
Target Address	(e.g., 1.2.3.4:160)
Target Timeout	1500 seconds (0 .. 2147483647)
Target Retry Count	3 (0 .. 255)
Target Tag List	
Target Param Entry	
Entry Storage	Volatile

Table 24 describes the items on the Target Address page.

Table 24 Target Address page items

Item and MIB association	Range	Description
☒		Deletes the row.
Target Name (snmpTargetAddrName)	1..32	Type a character string to create a target name.
Target Domain (snmpTargetAddrTDomain)	1..32	The transport type of the address contained in the snmpTargetAddrTAddress object.
Target Address (snmpTargetAddrTAddress)	XXX.XXX.XXX.XXX:XXX	Type a transport address in the format of an IP address, colon, and UDP port number. For example: 10.30.31.99:162 (see Figure 27 on page 85).
Target Timeout (snmpTargetAddrTimeout)	Integer	Type the number, in seconds, to designate as the maximum time to wait for a response to an inform notification before re-sending the “Inform” notification.
Target Retry Count (snmpTargetAddrRetryCount)	0..255	Type the default number of retires to be attempted when a response is not received for a generated message. An application may provide its own retry count, in which case the value of this object is ignored.
Target Tag List (snmpTargetAddrTagList)	1..20	Type the space-separated list of tag values to be used to select target addresses for a particular operation.
Target Parameter Entry (snmpTargetAddr)	1..32	Type a numeric string to identify an entry in the snmpTargetParamsTable. The identified entry contains SNMP parameters to be used when generated messages to be sent to this transport address
Entry Storage	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Target Address Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Target Address Table (Figure 27).

Note: This Target Address Table section of the Target Address page contains hyperlinks to the Target Parameter page. For more information, see “Configuring an SNMPv3 management target parameter” on page 87.

Deleting an SNMPv3 target address configuration

To delete an SNMPv3 target address configuration:

1. From the main menu, choose Configuration > SNMPv3 > Target Address.

   The Target Address page opens (Figure 27).

2. In the Target Address Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:

   - Click Yes to delete the target address configuration.
   - Click Cancel to return to the table without making changes.

Configuring an SNMPv3 management target parameter

SNMPv3 management target parameters are used during notification generation to specify the communication parameters used for exchanges with notification recipients.

You can view a table of existing SNMPv3 target parameter configurations, create SNMPv3 target parameters that associate notifications with particular recipients, and delete existing SNMPv3 target parameter configurations.

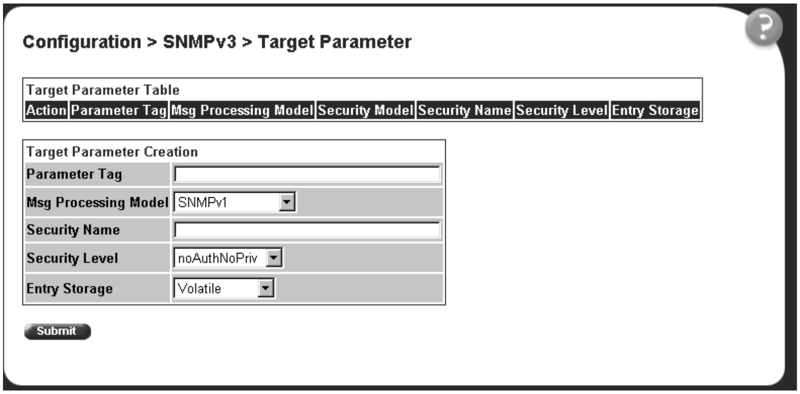
Creating an SNMPv3 target parameter configuration

To create an SNMPv3 target parameter configuration:

1. From the main menu, choose Configuration > SNMPv3 > Target Parameter.

   The Target Parameter page opens (Figure 28).

Figure 28 Target Parameter page



Configuration > SNMPv3 > Target Parameter

Target Parameter Table

Action	Parameter Tag	Msg Processing Model	Security Model	Security Name	Security Level	Entry Storage

Target Parameter Creation

Parameter Tag	
Msg Processing Model	SNMPv1
Security Name	
Security Level	noAuthNoPriv
Entry Storage	Volatile

Table 25 describes the items on the Target Parameter page.

Table 25 Target Parameter page items

Item	**Range**	**Description**
☒		Deletes the row.
Parameter Tag (snmpTargetParamsRowStatus)	1..32	Type a unique character string to identify the parameter tag.
Msg Processing Model (snmpTargetParamsMPModel)	(0) SNMPv1 (1) SNMPv2c (2) SNMPv2* (3) SNMPv3 /USM	Choose the message processing model to be used when generating SNMP messages using this entry.
Security Name (snmpTargetParamsSecuirtyName)	1..32	Type the principal on whose behalf SNMP messages are generated using this entry
Security Level (snmpTargetParamsSecuirtyLevel)	(1) noAuthNoPriv (2) authNoPriv	Choose the level of security to be used when generating SNMP messages using this entry
Entry Storage (snmpTargetParamsStorageType)	(1) Volatile (2) Non-Volatile	Choose your storage preference. Selecting Volatile requests information to be dropped (lost) when you turn the power off. Selecting Non-Volatile requests information to be saved in NVRAM when you turn the power off.

2 In the Target Parameter Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Target Parameter Table (Figure 28).

Deleting an SNMPv3 target parameter configuration

To delete an SNMPv3 target parameter configuration:

1. From the main menu, choose Configuration > SNMPv3 > Target Address.

   The Target Address page opens (Figure 27).

2. In the Target Parameter Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the target parameter configuration.
   - Click Cancel to return to the table without making changes.

Configuring SNMP traps

You can configure the IP address and community string for a new SNMP trap receiver, view a table of existing SNMP trap receiver configurations, or delete an existing SNMP trap receiver configuration(s).

Note: The SNMP Trap Receiver Table is an alternative to using the SNMPv3 Target Table and SNMPv3 Parameter Table. However, only SNMPv1 traps are configurable using this table.

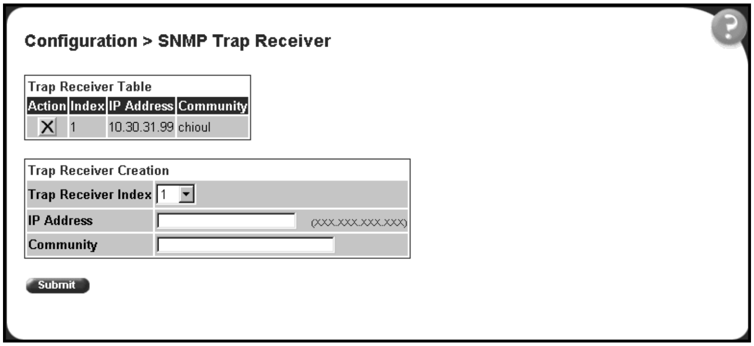
Creating an SNMP trap receiver configuration

To create an SNMP trap receiver configuration:

1. From the main menu, choose Configuration > SNMP Trap.

   The SNMP Trap Receiver page opens (Figure 29).

Figure 29 SNMP Trap Receiver page



Configuration > SNMP Trap Receiver

Trap Receiver Table

Action	Index	IP Address	Community
☒	1	10.30.31.99	chioul

Trap Receiver Creation

Trap Receiver Index	1
IP Address	(xxx.xxx.xxx.xxx)
Community	

Table 26 describes the items on the Trap Receiver Table and Trap Receiver Creation sections of the SNMP Trap Receiver page.

Table 26 SNMP Trap Receiver page items

Items	Range	Description
☒		Deletes the row.
Trap Receiver Index	1..4	Choose the number of the trap receiver to create or modify.
IP Address	XXX.XXX.XXX.XXX	Type the network address for the SNMP manager that is to receive the specified trap.
Community	0..32	Type the community string for the specified trap receiver.

2 In the Trap Receiver Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new entry appears in the Trap Receiver Table (Figure 29).

Deleting an SNMP trap receiver configuration

To delete SNMP trap receiver configurations:

1 From the main menu, choose Configuration > SNMP Trap.

The SNMP Trap Receiver page opens (Figure 29).

2 In the Trap Receiver Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the SNMP trap receiver configuration.
- Click Cancel to return to the table without making changes.

Configuring EAPOL-based security

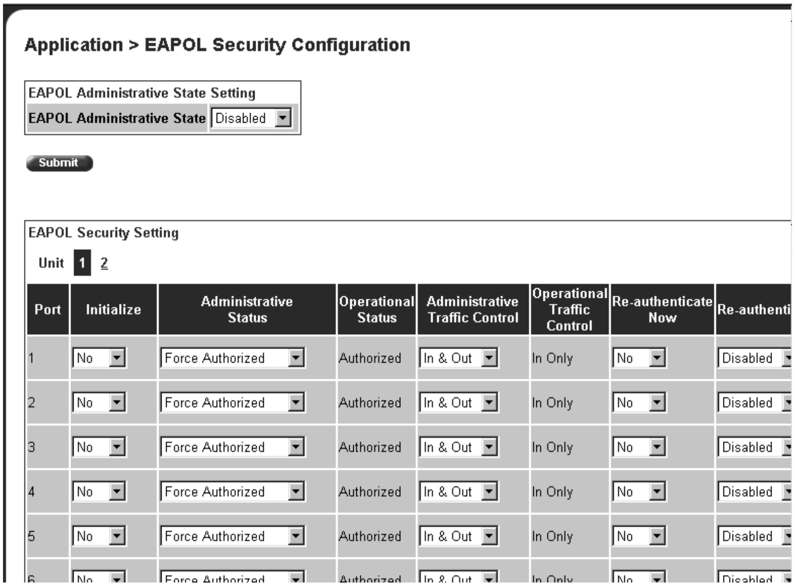
Beginning with software version 1.1, you can configure security based on the Extensible Authentication Protocol over LAN (EAPOL) protocol. Refer to *Using the Business Policy Switch 2000 Software Version 2.0***,** for more information EAPOL-based security.

To configure EAPOL:

1 From the main menu, choose Application > EAPOL Security.

The EAPOL Security Configuration page opens (Figure 30 and Figure 31). Use the scroll bar on the right to move down the page and the scroll bar on the bottom to move across the page.

Figure 30 EAPOL Security Configuration page (1 of 2)



Application > EAPOL Security Configuration

EAPOL Administrative State Setting

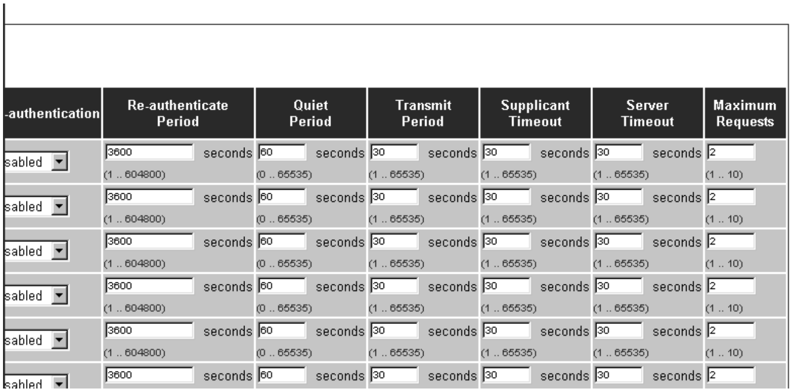
EAPOL Administrative State	Disabled

EAPOL Security Setting

Unit **1** 2

Port	Initialize	Administrative Status	Operational Status	Administrative Traffic Control	Operational Traffic Control	Re-authenticate Now	Re-authenti
1	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
2	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
3	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
4	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
5	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled
6	No	Force Authorized	Authorized	In & Out	In Only	No	Disabled

Figure 31 EAPOL Security Configuration page (2 of 2)



-authentication	Re-authenticate Period	Quiet Period	Transmit Period	Supplicant Timeout	Server Timeout	Maximum Requests
sabled	3600 seconds (1 .. 604800)	60 seconds (0 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	2 (1 .. 10)
sabled	3600 seconds (1 .. 604800)	60 seconds (0 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	2 (1 .. 10)
sabled	3600 seconds (1 .. 604800)	60 seconds (0 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	2 (1 .. 10)
sabled	3600 seconds (1 .. 604800)	60 seconds (0 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	2 (1 .. 10)
sabled	3600 seconds (1 .. 604800)	60 seconds (0 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	30 seconds (1 .. 65535)	2 (1 .. 10)
sabled	3600 seconds	60 seconds	30 seconds	30 seconds	30 seconds	2

Table 27 describes the fields on the EAPOL Security Configuration page.

Table 27 EAPOL Security Configuration page fields

Section	Item	Range	Description
EAPOL Administrative State Setting	EAPOL Administrative State	(1) Enabled (2) Disabled	Enables or disables EAPOL-based security.
EAPOL Security Setting	Unit		Displays the unit you are viewing.
	Port	1 to 28	Displays the port number.
	Initialize	(1) Yes (2) No	Activates EAPOL state on this port.
	Administrative Status	(1) Force Unauthorized (2) Auto (3) Force Authorized	Allows you to set the EAPOL authorization status: • Force Unauthorized—Always unauthorized • Auto—Status depends on EAP authentication results • Force Authorized—Always authorized
	Operational Status	(1) Authorized (2) Unauthorized	Displays the current authorization status.
	Administrative Traffic Control	(1) In & Out (2) In Only	Allows you to set EAPOL authentication either for incoming and outgoing traffic or for incoming traffic only.
	Operational Traffic Control	(1) In & Out (2) In Only	Displays the current administrative traffic control setting.
	Re-authenticate Now	(1) Yes (2) No	Allows you to activate EAPOL authentication immediately, without waiting for the re-authentication period to expire.
	Re-authentication	(1) Enabled (2) Disabled	Allows you to repeat EAPOL authentication according to the time value specified in Re-authentication Period field.
	Re-authentication Period	1..604800	With Re-authentication enabled, allows you to specify the time period between successive EAPOL authentications.
	Quiet Period	0..65535	Allows you to specify the time interval between an authentication failure and the start of a new authentication attempt.
	Transmit Period	1..65535	Allows you to specify how long the switch waits for the supplicant to respond to EAP Request/Identity packets.
	Supplicant Timeout	1..65535	Allows you to specify how long the switch waits for the supplicant to respond to all EAP packets, except EAP Request/Identity packets.
	Server Timeout	1..65535	Allows you to specify how long the switch waits for the RADIUS server to respond to all EAP packets.
	Maximum Requests	1..10	Allows you to specify the number of times the switch attempts to resend EAP packets to a supplicant.

2. Complete fields as described in the table.
3. Click Submit.

Managing remote access by IP address

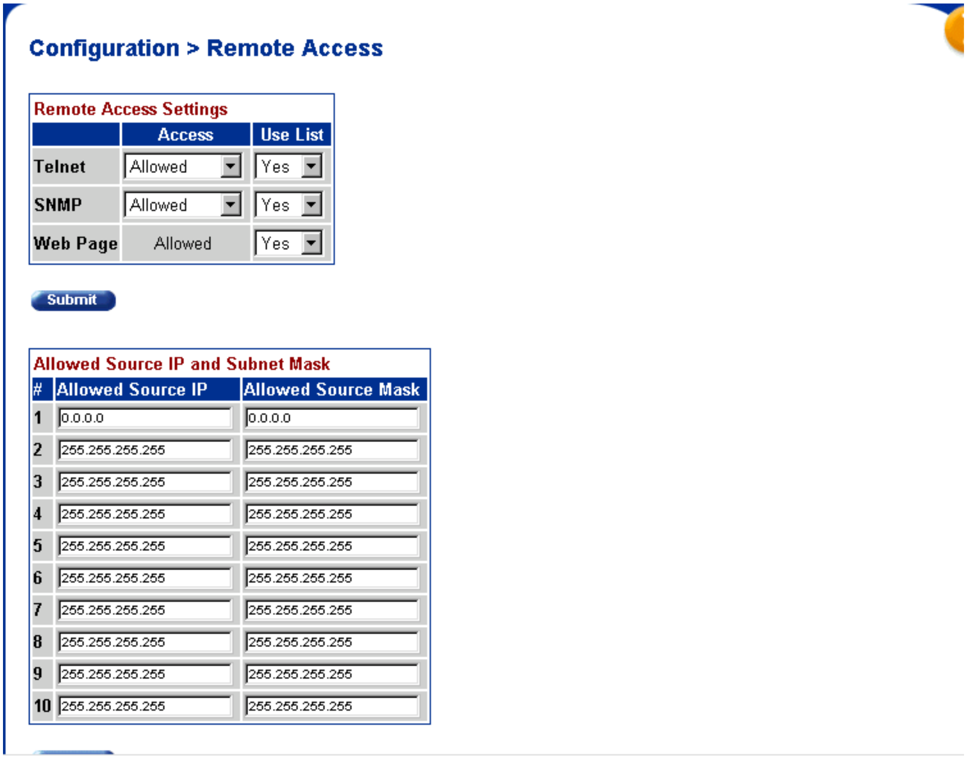
Beginning with software version 1.2, you can configure the remote access you allow. You can specify up to 10 IP addresses to allow Web access, SNMP access, or Telnet access to the BPS 2000.

To configure remote access using the Web-based management system:

1. From the main menu of the Business Policy Switch 2000 Web-based Manager, choose Configuration > Remote Access.

   The Remote Access page opens (Figure 32).

Figure 32 Remote Access page



Configuration > Remote Access

Remote Access Settings

	Access	Use List
Telnet	Allowed	Yes
SNMP	Allowed	Yes
Web Page	Allowed	Yes

Allowed Source IP and Subnet Mask

#	Allowed Source IP	Allowed Source Mask
1	0.0.0.0	0.0.0.0
2	255.255.255.255	255.255.255.255
3	255.255.255.255	255.255.255.255
4	255.255.255.255	255.255.255.255
5	255.255.255.255	255.255.255.255
6	255.255.255.255	255.255.255.255
7	255.255.255.255	255.255.255.255
8	255.255.255.255	255.255.255.255
9	255.255.255.255	255.255.255.255
10	255.255.255.255	255.255.255.255

Table 28 describes the fields on the Remote Access page.

Table 28 Remote Access page fields

Section	Item	Range	Description
Remote Access Settings	Telnet/Access	(1)Allowed (2) Disallowed	Allows Telnet access.
	Telnet/Use List	(1) Yes (2) No	Restricts Telnet access to the specified 10 source IP addresses.
	SNMP/Access	(1)Allowed (2) Disallowed	Allows SNMP access.
	SNMP/Use List	(1) Yes (2) No	Restricts SNMP access to the specified 10 source IP addresses.
	Web Page/Access		Displays allowed Web access.

Table 28 Remote Access page fields (continued)

Section	Item	Range	Description
	Web/Use List	(1) Yes (2) No	Restricts Web access to the specified 10 source IP addresses.
Allowed Source IP and Subnet Mask	Allowed Source IP	XXX.XXX.XXX.XXX	Enter the source IP address you want to allow switch access.
	Allowed Source Mask	XXX.XXX.XXX.XXX	Enter the source IP mask you want to allow switch access.

2 Complete fields as described in the table.

3 Click Submit.

Configuring MAC address-based security

Beginning with software version 1.1, the MAC address-based security system allows you to specify a range of system responses to unauthorized network access to your switch with the Web-based management system.

The system response can range from sending a trap to disabling the port. The network access control is based on the MAC source addresses (SAs) of the authorized stations. You can specify a list of up to 448 MAC SAs that are authorized to access the switch. You can also specify the ports that each MAC SA is allowed to access. The options for allowed MAC SA port access include: NONE, ALL, and single or multiple ports that are specified in a list, for example, 1-4, 6, 9, and so forth. You must also include the MAC SA of any router connected to any secure ports.

When the switch software detects an SA security violation, the response can be to send a trap, turn on destination address (DA) filtering for all SAs, disable the specific port, or any combination of these three options.

Beginning with software version 2.0, you can configure the BPS 2000 to drop all packets having a specified MAC destination address (DA). You can create a list of up to 10 MAC DAs you want to filter.The packet with the specified MAC DA will be dropped regardless of the ingress port, source address (SA) intrusion, or VLAN membership.

Note: Ensure that you do not enter the MAC address of the switch or stack you are working on.

This feature is available only with BPS2000 software version 2.0 and higher. Also, this feature is unavailable on the BayStack 450 or 410 switches. In a Hybrid stack, only the BPS 2000 will filter the specified MAC DAs.

Note: After configuring the switch for MAC address-based security, you must enable the ports you want, using the Port Configuration page.

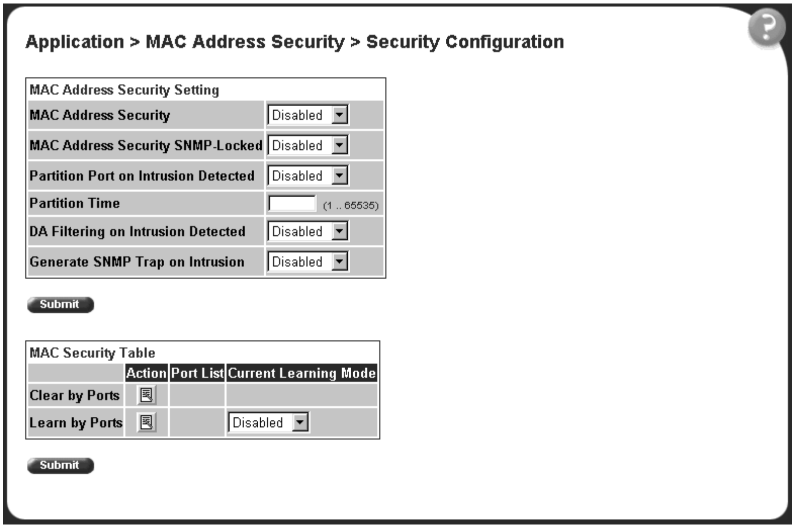
Configuring MAC address-based security

To configure MAC address-based security using the Web-based management system:

1 From the main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 33).

Figure 33 Security Configuration page



Application > MAC Address Security > Security Configuration

MAC Address Security Setting	
MAC Address Security	Disabled
MAC Address Security SNMP-Locked	Disabled
Partition Port on Intrusion Detected	Disabled
Partition Time	(1 .. 65535)
DA Filtering on Intrusion Detected	Disabled
Generate SNMP Trap on Intrusion	Disabled

MAC Security Table

	Action	Port List	Current Learning Mode
Clear by Ports			
Learn by Ports			Disabled

Table 29 describes the items on the Security Configuration page.

Table 29 Security Configuration page items

Section	Item	Range	Description
MAC Address Security Setting	MAC Address Security	(1) Enabled (2) Disabled	Enables the MAC address security features.
	MAC Address Security SNMP-Locked	(1) Enabled (2) Disabled	Enables locking SNMP, so that you cannot use SNMP to modify the MAC address security features.
	Partition Port on Intrusion Detected	(1) Forever (2) Enabled (3) Disabled	Configures how the switch reacts to an intrusion event: • Forever—The port is disabled and remains disabled (partitioned) until reset. The port does not reset after the Partition Time elapses. • Enabled—The port is disabled, then automatically reset to enabled after the time specified in the Partition Time field elapses. • Disabled—The port remains enabled, even if an intrusion event is detected.

Table 29 Security Configuration page items (continued)

Section	Item	Range	Description
	Partition Time	1 to 65535	Sets the time to partition a port on intrusion. Note: Use this field only if the Partition Port on Intrusion Detected field is set to Enabled.
	DA Filtering on Intrusion Detected	(1) Enabled (2) Disabled	Enables you to isolate the intruding node (discard) the packets.
	Generate SNMP Trap on Intrusion	(1) Enabled (2) Disabled	Enables generation of an SNMP when an intrusion is detected.
MAC Security Table/ Clear by Ports	Action	✎	Allows you to clear specific ports from participation in the MAC address security features.
	Port List		Will be blank.
	Current Learning Mode		Will be blank.
MAC Security Table/ Learn by Ports	Action	✎	Allows you to identify ports that will learn incoming MAC addresses. All source MAC addresses of any packets received on a specified port(s) are added to the MAC Security Table (maximum of 448 MAC addresses allowed).
	Port List		Displays all the ports that will learn incoming MAC address to detect intrusions (unallowed MAC addresses).
	Current Learning Mode	(1) Enabled (2) Disabled	Enables learning.

2. On the Security Configuration page, type information in the text boxes, or select from a list.
3. Click Submit.

Configuring ports

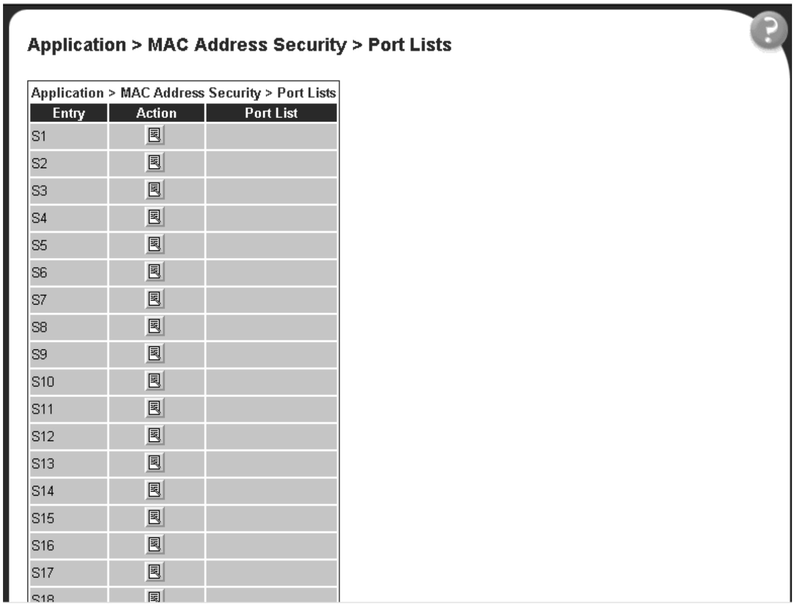
In this section, you create a list of ports, and you can add ports to or delete ports from each list.

To activate an entry or add or delete ports to a list:

1. From the main menu, choose Application > MAC Address Security > Port Lists.

   The Port Lists page opens (Figure 34).

Figure 34 Port Lists page



Application > MAC Address Security > Port Lists

Application > MAC Address Security > Port Lists

Entry	Action	Port List
S1	▤	
S2	▤	
S3	▤	
S4	▤	
S5	▤	
S6	▤	
S7	▤	
S8	▤	
S9	▤	
S10	▤	
S11	▤	
S12	▤	
S13	▤	
S14	▤	
S15	▤	
S16	▤	
S17	▤	
S18	▤	

Table 30 describes the items on the Ports Lists page.

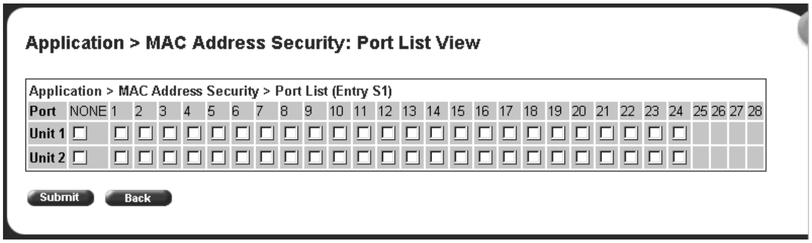
Table 30 Ports Lists page items

Item	**Range**	**Description**
Entry		These are the lists of ports.
Action	▤	Allows you to add or delete ports to the lists.
Port List		Displays which ports are associated with each list.

2 To add or delete ports to a list, click the icon in the Action column in the list row you want.

The Port List View, Port List page opens (Figure 35).

Figure 35 Port List View, Port List page



Application > MAC Address Security: Port List View

Application > MAC Address Security > Port List (Entry S1)

Port	NONE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				

a Click the ports you want to add to the selected list or click None.

b To delete a port from a list, uncheck the box by clicking it.

c Click Submit.

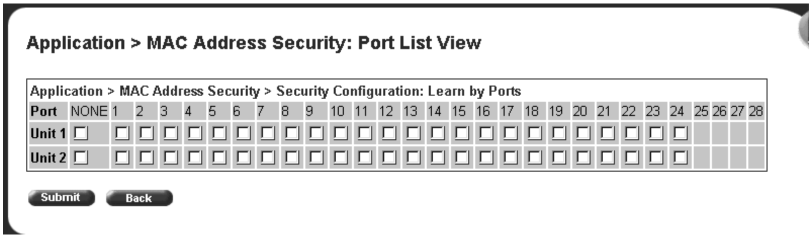
3 From the main menu, choose Application > MAC Address Security > Security Configuration.

The Security Configuration page opens (Figure 33).

4 In the MAC Security Table section, click the icon in the Action column of the Learn By Ports row.

The Port List View, Learn by Ports page opens (Figure 36).

Figure 36 Port List View, Learn by Ports page



Application > MAC Address Security: Port List View

Application > MAC Address Security > Security Configuration: Learn by Ports

Port	NONE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				

a Click the ports through which you want the switch to learn MAC addresses or click None.

b If you want that port to no longer learn MAC addresses, click the checked box to uncheck it.

   c Click Submit.

5 In the MAC Security Table section, choose Enabled in the Current Learning Mode column of the Learn By Ports row.

6 Click Submit.

Note: You cannot include any of the port values you have chosen for the secure ports field.

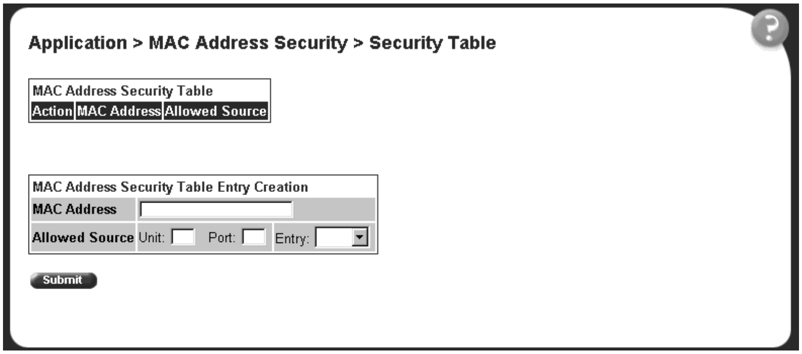
Adding MAC addresses

To add MAC address to the MAC address-based security system:

1 In the main menu, choose Applications > MAC Address Security > Security Table.

It may take awhile for the required addresses to be learned. Then, the Security Table page opens (Figure 37).

Figure 37 Security Table page



Application > MAC Address Security > Security Table

MAC Address Security Table

Action	MAC Address	Allowed Source

MAC Address Security Table Entry Creation

MAC Address	
Allowed Source	Unit: Port: Entry:

Note: Using this page, you instruct the switch to allow the specified MAC address access *only* through the specified port or port list.

Table 31 describes the items on the Security Table page.

Table 31 Security Table page items

Section	Item	Range	Description
MAC Address Security Table	Action	☒	Allows you to delete a MAC address.
	Address		Displays the MAC address.
	Allowed Source	(1) Unit/Port (2) Entry	Displays the entry through which the MAC address is allowed.
MAC Address Security Table Entry Creation	MAC Address		Enter the MAC address you want to allow to access the switch.
	Allowed Source		Select the unit and port through which the MAC address is allowed.
	Entry		Select the port list through which the MAC address is allowed.

2 Complete fields as described in the table.

Note: If you choose an Entry as the Allowed Source, you must have configured that specific entry on the Port View List, Port List page.

3 On the Security Table page, type information in the text boxes, or select from a list.

4 Click Submit.

Note: Be certain to include the MAC address for the default LAN router as an allowed source MAC address.

Clearing ports

You can clear all information from the specified port(s) for the list of ports that learn MAC addresses. If Learn by Ports is enabled, the specified ports will begin again to learn the MAC addresses.

To clear information from selected ports:

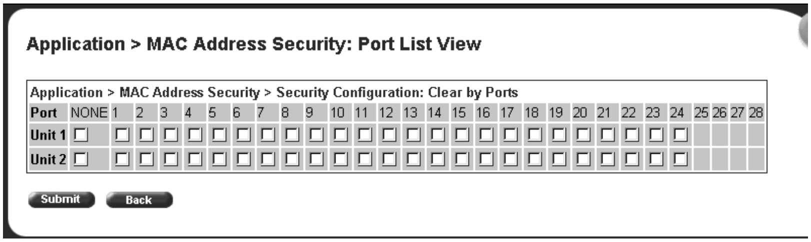
1 From the main menu, choose Application > MAC Address Security > Security Configuration.

  The Security Configuration page opens (Figure 33).

2 In the MAC Security Table section, click the icon in the Action column of the Clear By Ports row.

  The Port List View, Clear by Ports page opens (Figure 38).

Figure 38 Port List View, Clear by Ports page



Application > MAC Address Security: Port List View

Application > MAC Address Security > Security Configuration: Clear by Ports

Port	NONE	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				

3 Select the ports you want to clear or click None.

4 Click Submit.

Note: When you specify a port (or ports) to be cleared using this field, the specific port (or ports) will be cleared for each of the entries listed in the MAC Address Security Table. If you totally clear the allowed Source Port(s) field (leaving a blank field) for an entry, the associated MAC address for that entry is also cleared.

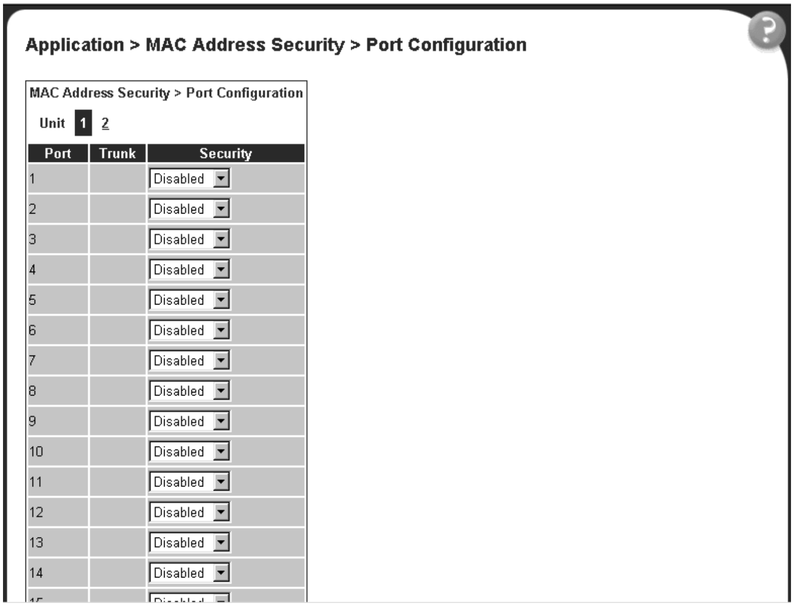
Enabling security on ports

To enable or disable MAC address-based security on the port:

1 From the main menu, choose Application > MAC Address Security > Port Configuration.

  The Port Configuration page opens (Figure 39).

Figure 39 Port Configuration page



Application > MAC Address Security > Port Configuration

MAC Address Security > Port Configuration

Unit **1** 2

Port	Trunk	Security
1		Disabled
2		Disabled
3		Disabled
4		Disabled
5		Disabled
6		Disabled
7		Disabled
8		Disabled
9		Disabled
10		Disabled
11		Disabled
12		Disabled
13		Disabled
14		Disabled

Table 32 describes the items on the Port Configuration page.

Table 32 Port Configuration page items

Item	Range	Description
Unit	1 to 8	Displays the unit number of the ports shown in the table.
Port	1 to 28	Lists each port on the unit.
Trunk	Blank, 1 to 6	Displays the MultiLink Trunk that the port belongs to.
Security	(1) Enabled (2) Disabled	Enables MAC address-based security on that port. Note: You must configure the port for MAC address-based security before enabling the security.

Deleting ports

You can delete ports from the security system in a variety of ways:

- In the Ports List View, Port List page (Figure 35), click on the checkmark of a selected port to delete that port from the specified port list.

- In the Ports List View, Learn by Ports page (Figure 36), click on the checkmark of a selected port to remove that port from those that learn MAC addresses.
- In the Port Configuration page (Figure 39), click Disabled to remove that port from the MAC address-based security system; it will disable all MAC address-based security on that port.

Filtering MAC destination addresses

To drop all packets from a specified MAC destination address (DA):

1 From the main menu, choose Application > MAC Address Security > DA MAC Filtering.

The DA MAC Filtering page opens (Figure 40).

Figure 40 DA MAC Filtering page

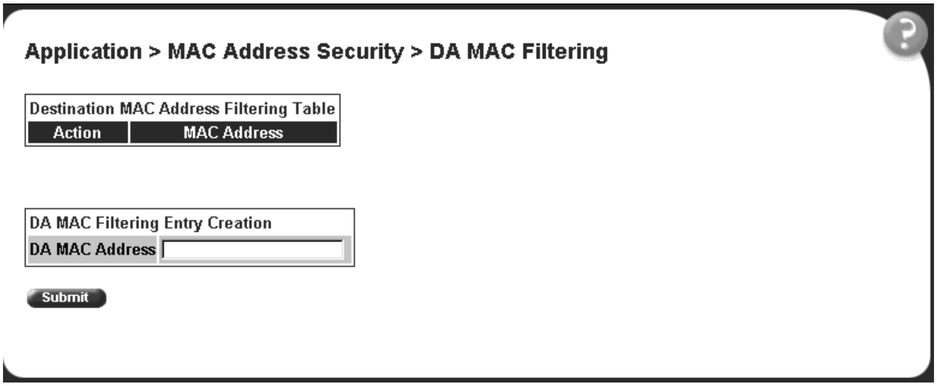

Application > MAC Address Security > DA MAC Filtering
Destination MAC Address Filtering Table
Action
MAC Address
DA MAC Filtering Entry Creation
DA MAC Address
Submit

Table 33 describes the items on the DA MAC Filtering page.

Table 33 DA MAC Filtering page items

Section	Item	Range	Description
Destination MAC Address Filtering Table	Action	☒	Allows you to delete a MAC DA you are filtering.

Table 33 DA MAC Filtering page items

Section	Item	Range	Description
	MAC Address	1 -10	Displays list of MAC DAs you want filtered.
DA MAC Filtering Entry Creation	DA MAC Address	XX:XX:XX:XX:XX:XX	Enter the MAC DA you want to filter.

Note: Ensure that you do not enter the MAC address of the management station.

2 In the DA MAC Filtering Entry Creation area, enter the MAC DA you want to filter.

You can list up to 10 MAC DAs to filter.

3 Click Submit.

The system returns you to the DA MAC FIltering page (Table 40) with the new DA listed in the table.

Deleting MAC DAs

To delete a MAC DA:

1 From the main menu, choose Application > MAC Address Security > DA MAC Filtering.

The DA MAC Filtering page opens (Figure 40).

2 In the Destination MAC Address Filtering Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the target parameter configuration.
- Click Cancel to return to the table without making changes.

Viewing learned MAC addresses by VLAN

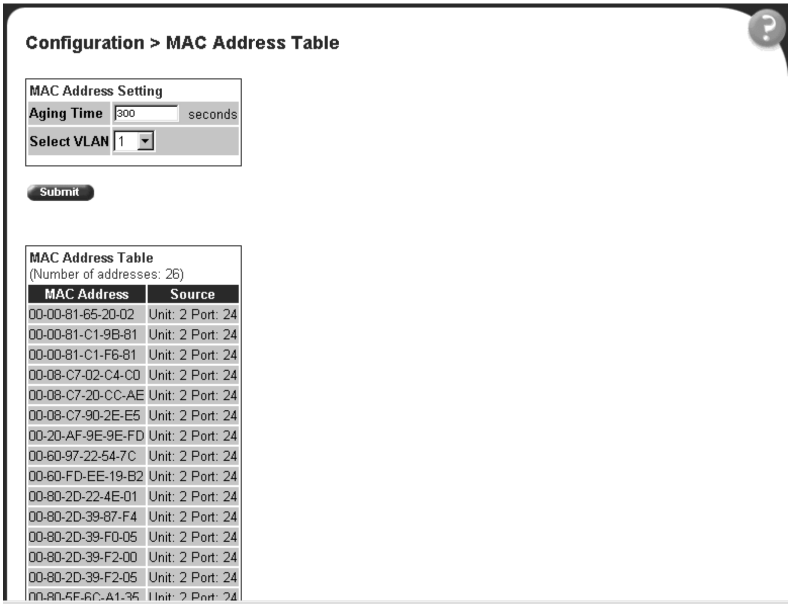
You can view MAC addresses and their associated port or trunk that the switch or stack configuration has learned, based on the VLAN you select.

To view learned MAC addresses and their associated port or trunk:

1 From the main menu, choose Configuration > MAC Address Table.

The MAC Address Table page opens (Figure 41).

Figure 41 MAC Address Table page



MAC Address Setting

Aging Time: 300 seconds

Select VLAN: 1

MAC Address Table
(Number of addresses: 26)

MAC Address	Source
00-00-81-65-20-02	Unit: 2 Port: 24
00-00-81-C1-9B-81	Unit: 2 Port: 24
00-00-81-C1-F6-81	Unit: 2 Port: 24
00-08-C7-02-C4-C0	Unit: 2 Port: 24
00-08-C7-20-CC-AE	Unit: 2 Port: 24
00-08-C7-90-2E-E5	Unit: 2 Port: 24
00-20-AF-9E-9E-FD	Unit: 2 Port: 24
00-60-97-22-54-7C	Unit: 2 Port: 24
00-60-FD-EE-19-B2	Unit: 2 Port: 24
00-80-2D-22-4E-01	Unit: 2 Port: 24
00-80-2D-39-87-F4	Unit: 2 Port: 24
00-80-2D-39-F0-05	Unit: 2 Port: 24
00-80-2D-39-F2-00	Unit: 2 Port: 24
00-80-2D-39-F2-05	Unit: 2 Port: 24
00-80-5F-6C-A1-35	Unit: 2 Port: 24

Table 34 describes the items on the MAC Address Table page.

Table 34 MAC Address Table page items

Section	Item	Range	Description
MAC Address Setting	Aging Time	10..1000000	Type the timeout period, in seconds, for aging out dynamically learned forwarding information. If the entry is inactive for a period of time that exceeds the specified aging time, the address is removed. Note: Nortel Networks recommends that you use the default value of 300 seconds.
	Select VLAN	1..256	Choose the VLAN on which to view learned MAC addresses.
MAC Address Table	MAC Address		The unicast MAC address for which the bridge has forwarding and/or filtering information.
	Source		The source of the discovered MAC address.

2 In the MAC Address Setting section, choose the aging time and VLAN you want to view learned MAC addresses on.

3 Click Submit.

Your request is displayed in the MAC Address Table (Figure 41).

Locating a specific MAC address

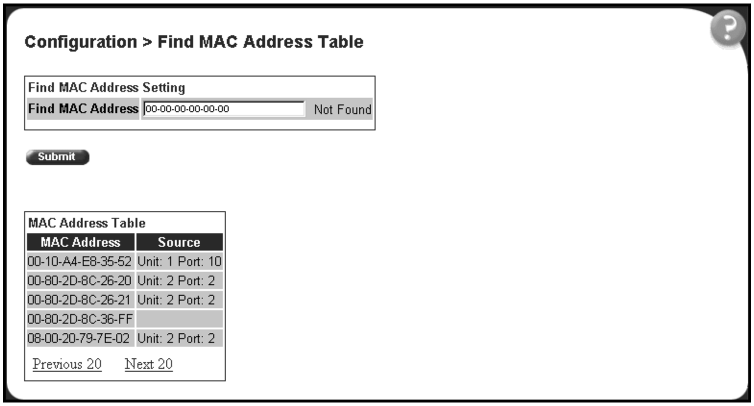
You can search for a specific MAC address among all the MAC addresses learned from all the VLANs. This is a useful tool for finding whether or not a switch has learned a particular address.

To locate a specific MAC addresses:

1 From the main menu, choose Configuration > Find MAC Address.

The Find MAC Address page opens (Figure 42).

Figure 42 Find MAC Address Table page



Configuration > Find MAC Address Table

Find MAC Address Setting

Find MAC Address	00-00-00-00-00-00	Not Found

MAC Address Table

MAC Address	Source
00-10-A4-E8-35-52	Unit: 1 Port: 10
00-80-2D-8C-26-20	Unit: 2 Port: 2
00-80-2D-8C-26-21	Unit: 2 Port: 2
00-80-2D-8C-36-FF	
08-00-20-79-7E-02	Unit: 2 Port: 2

Table 34 on page 109 describes the items on the Find MAC Address Table page.

2. In the MAC Address Setting section, type the MAC address you want to search for.
3. Click Submit to enter the request.

   If the address is located, it is shown in the first row in the MAC Address Table section. If the address is not located, the system response “Not Found” is shown to the right of the Find MAC Address input field.

Configuring port's autonegotiation, speed, duplex, status, and alias

You can configure a specific switch port or all switch ports to autonegotiate for the highest available speed of the connected station or you can set the speed for selected switch ports. Autonegotiation is not supported on fiber optic ports.

Note: You cannot *disable* autonegotiation using the BPS2000-1GT or BPS2000-2GT MDA ports; you cannot *enable* autonegotiation using the BPS2000-2GE MDA ports.Use the High Speed Flow control page to work with autonegotiation and gigabit ports.

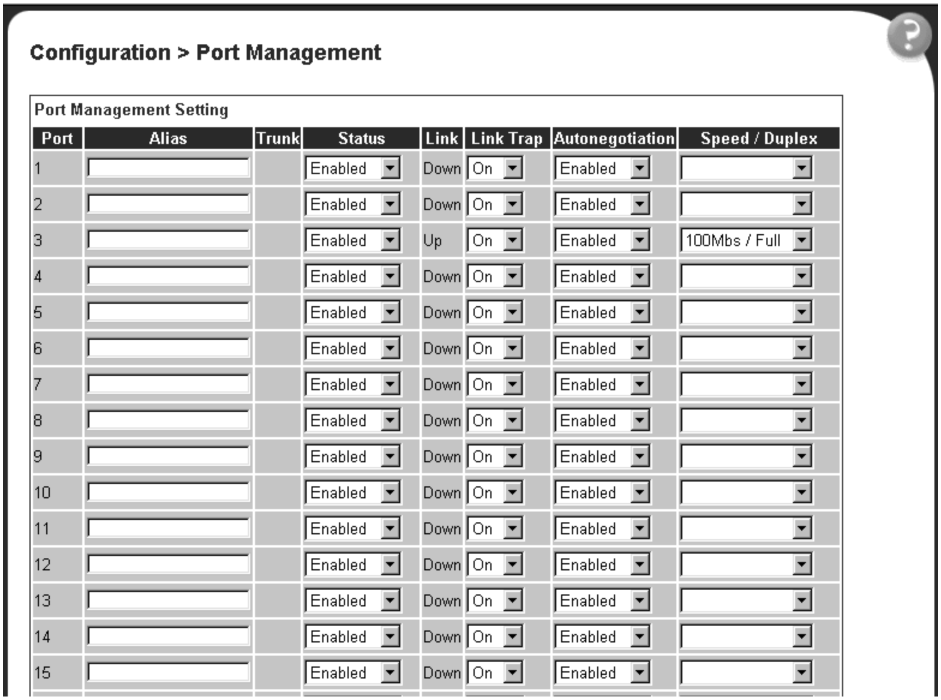
With software version 2.0, you can name each port, or assign an alias to it, using 27 alphanumeric characters.

To configure a switch port's alias, status, autonegotiation and speed/duplex:

1. From the main menu, choose Configuration > Port Management.

   The Port Management page opens (Figure 43).

Figure 43 Port Management page



Configuration > Port Management

Port Management Setting

Port	Alias	Trunk	Status	Link	Link Trap	Autonegotiation	Speed / Duplex
1			Enabled	Down	On	Enabled	
2			Enabled	Down	On	Enabled	
3			Enabled	Up	On	Enabled	100Mbs / Full
4			Enabled	Down	On	Enabled	
5			Enabled	Down	On	Enabled	
6			Enabled	Down	On	Enabled	
7			Enabled	Down	On	Enabled	
8			Enabled	Down	On	Enabled	
9			Enabled	Down	On	Enabled	
10			Enabled	Down	On	Enabled	
11			Enabled	Down	On	Enabled	
12			Enabled	Down	On	Enabled	
13			Enabled	Down	On	Enabled	
14			Enabled	Down	On	Enabled	
15			Enabled	Down	On	Enabled	

Table 35 describes the items on the Port Management page.

Table 35 Port Management page items

Item	Range	Description
Port		The switch port number of the corresponding row. To select the switch row, click the check box to the right. The values that you set in each switch row affect all switch ports and, when the switch is part of a stack, the values that set in the stack row affect all ports in the entire stack (except the gigabit media dependent adaptor (MDA) ports or fiber optic ports when installed). For information on setting high speed flow control for MDAs, see "Configuring high speed flow control" on page 114.
Alias	27 alphanumeric characters	Displays the name, or alias, you assigned the port. To assign a name or to change the name, enter up to 26 alphanumeric characters.
Trunk		The trunk group that the switch port belongs to as specified in the Trunk Member fields on the MultiLink Trunk page. For more information, see "Configuring MultiLink Trunk (MLT) members" on page 202.
Status	(1) Enabled (2) Disabled	Choose to enable or disable the port. You can also use this field to control access to any switch port. The default setting is Enabled.
Link		The current link state of the corresponding port as follows: • Up: The port is connected and operational • Down: The port is not connected or is not operational.
Link/Trap	(1) On (2) Off	Choose to control whether link up/down traps are sent to the configured trap sink from the switch. The default setting is On.
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. Choosing to enable autonegotiation sets the corresponding port speed to match the best service provided by the connected station, up to 100Mb/s in full-duplex mode. **NOTE**: This field is disabled for all fiber optic ports. Additionally, you cannot disable this field for the ports on the BPS2000-1GT and BPS2000-2GT MDAs. Use the High Speed Flow Control Configuration screen (next) to set autonegotiation for all gigabit ports. The default setting is Enabled.

Table 35 Port Management page items

Item	Range	Description
Speed / Duplex	(1) 10Mbs / Half (2) 10Mbs / Full (3) 100Mbs / Half (4) 100Mbs / Full (5) 1000Mbs / Full	Choose the Ethernet speed you want the port to support. **NOTE**: Fiber optic ports can only be set to 100 Mb/s/Half or 100 Mb/s/Full. Use the High Speed Flow Control Configuration screen (next) to set autonegotiation for all gigabit ports. The default setting is 100Mbs/Half when autonegotiation is disabled and 1000 Mb/s full-duplex for gigabit ports only.
	Note: Disabling ports that are trunk members automatically disables all ports within that trunk.	

2 In the upper-left hand corner, click on the unit number of the policy switch to manage.

The page is updated with the information for the selected switch.

3 In the port row of your choice, select from the lists.

4 Click Submit.

Configuring high speed flow control

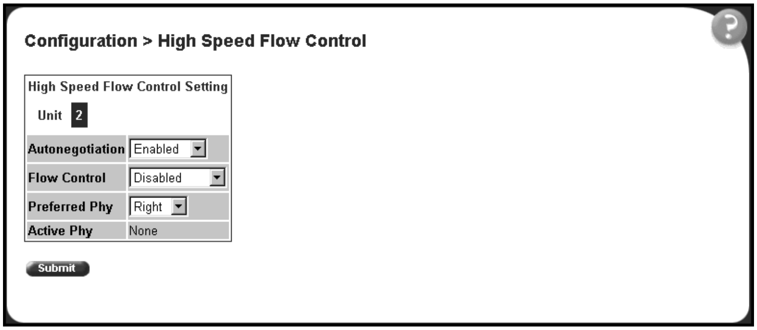
You can set switch port parameters for gigabit Ethernet media dependent adapters (MDAs). Use this screen to set autonegotiation for all gigabit ports.

To configure high speed flow control:

1 From the main menu, choose Configuration > High Speed Flow Control.

The High Speed Flow Control page opens (Figure 44).

Figure 44 High Speed Flow Control page



Configuration > High Speed Flow Control

High Speed Flow Control Setting

Unit 2

Autonegotiation	Enabled
Flow Control	Disabled
Preferred Phy	Right
Active Phy	None

Table 36 describes the items on the High Speed Flow Control page.

Table 36 High Speed Flow Control page items

Item	Range	Description
Autonegotiation	(1) Enabled (2) Disabled	Choose to enable or disable the autonegotiation feature. **NOTE**: This field is disabled for all fiber optic ports. Additionally, you cannot disable this field for the ports on the BPS2000-1GT and BPS2000-2GT MDAs. When enabled, the port advertises support for flow control autonegotiation.
Flow Control	(1) Enabled (2) Symmetric (3) Asymmetric	Choose your flow control preference to control traffic and avoid congestion on the gigabit MDA port. Note: Ensure that the settings are the same for both sides of the link.
Preferred Phy	(1) Left (2) Right	Choose the preferred physical port. The port not selected automatically reverts to a backup physical port. **NOTE**: This field may not appear, depending on the MDA you are using.
Active Phy		The current operating physical port. The physical port options are left or right. **NOTE**: This field may not appear, depending on the MDA you are using.

2 In the upper-left hand corner, click on the unit number of the gigabit MDA to configure.

3 Select from the lists.

4 Click Submit.

Downloading switch images

You can download the BPS 2000 software image that is located in non-volatile flash memory. To download the BPS 2000 software image, a properly configured Trivial File Transfer Protocol (TFTP) server must be present in your network, and the policy switch must have an IP address. To learn how to configure the switch or stack IP address, refer to "Configuring BootP, IP, and gateway settings" on page 64.

Caution: Do not interrupt power to the device during the software download process. A power interruption can corrupt the firmware image.

In addition to downloading switch images, this section covers the following topics:

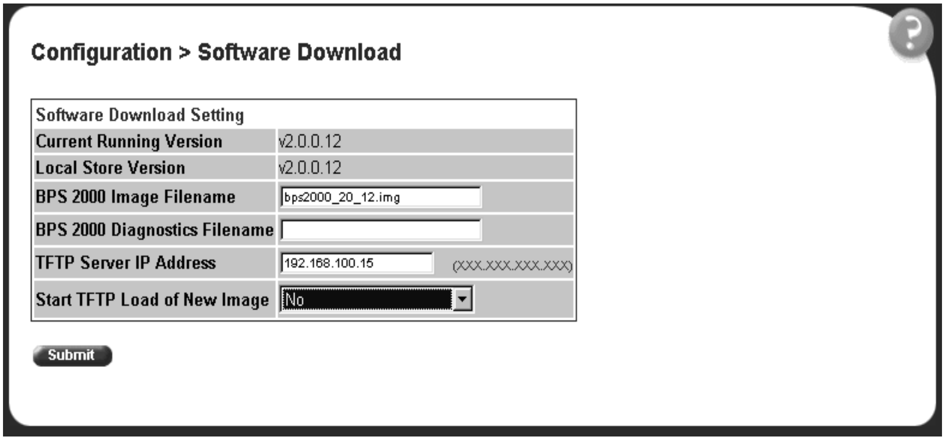
- "Observing LED indications," next
- "Upgrading software" on page 119

To download a switch image:

1 From the main menu, choose Configuration > Software Download.

The Software Download page opens (Figure 45 and Figure 46).

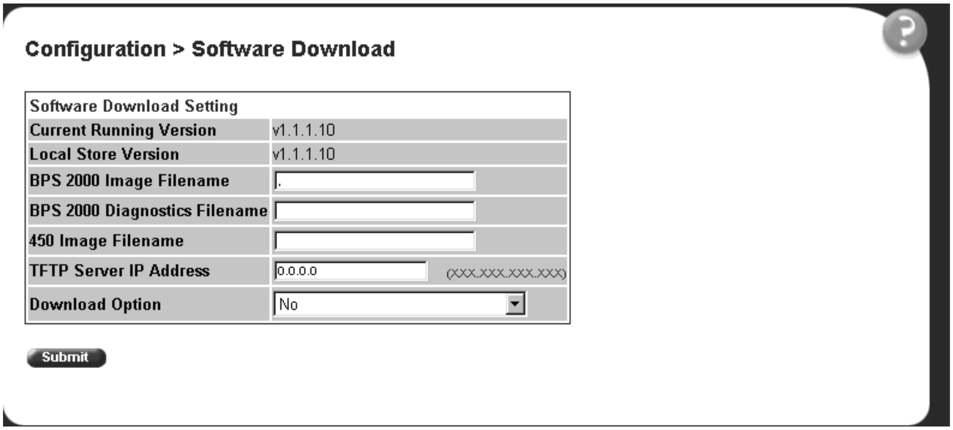
Figure 45 Software Download page for a Pure BPS 2000 stack



Configuration > Software Download

Software Download Setting	
Current Running Version	v2.0.0.12
Local Store Version	v2.0.0.12
BPS 2000 Image Filename	bps2000_20_12.img
BPS 2000 Diagnostics Filename	
TFTP Server IP Address	192.168.100.15 (XXX.XXX.XXX.XXX)
Start TFTP Load of New Image	No

Figure 46 Software Download page for a Hybrid stack



Configuration > Software Download

Software Download Setting	
Current Running Version	v1.1.1.10
Local Store Version	v1.1.1.10
BPS 2000 Image Filename	.
BPS 2000 Diagnostics Filename	
450 Image Filename	
TFTP Server IP Address	0.0.0.0 (XXX.XXX.XXX.XXX)
Download Option	No

Table 37 describes the items on the Software Download page.

Table 37 Software Download page items

Item	Range	Description
Current Running Version		The version of the current running software.
Local Store Version		The local version of the software in the flash memory.
BPS 2000 Image Filename	1..30	Type the software image load filename.
BPS 2000 Diagnostics Filename	1..30	Type the diagnostics filename.
450 Image Filename	1..30	Type the 450 image filename.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of your TFTP load host.
Start TFTP Load of New Image (in Pure BPS2000 mode) Download Option (in Hybrid mode)	(1) No (2) BPS 2000 Image (3) BPS 200 Diagnostics (4) 450/410 Image (5) BPS 2000 and 450/410 Images	Choose the software image to load.

2 Type information in the text boxes, or select from a list. (Refer to "Upgrading software" on page 119 for instructions.)

3 Click Submit.

The software download process automatically completes without user intervention. The process erases the contents of flash memory and replaces it with a new software image. Take care not to interrupt the download process until after it runs to completion (the process can take up to 10 minutes, depending on network conditions).

When the download process is complete, the switch automatically resets and the new software image initiates a self-test.

During the download process, the Business Policy Switch is not operational. You can monitor the progress of the download process by observing the LED indications.

Observing LED indications

Table 38 describes the LED indications during the software download process.

➡ **Note:** The LED indications described in Table 38 apply to a 24-port switch model. Although a 12-port switch provides *similar* LED indications, the LED indication sequence is associated within the 12-port range.

Table 38 LED Indications during the software download process

Phase	Description	LED Indications
1	The switch downloads the new software image.	**100 Mb/s port status LEDs (ports 18 to 24 only):** The LEDs begin to turn on in succession beginning with port 24, which indicates the progress of the download process. When LEDs 18 to 24 are all on, the switch has received the new software image successfully.
2	The switch erases the flash memory.	**100 Mb/s port status LEDs (ports 1 to 12 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that various sectors of the switch's flash memory are being erased. When LEDs 1 to 12 are all on, the switch's flash memory has been erased.

Table 38 LED Indications during the software download process (continued)

Phase	Description	LED Indications
3	The switch programs the new software image into the flash memory.	**100 Mb/s port status LEDs (ports 1 to 8 only):** The LEDs begin to turn on in succession beginning with port 1, which indicates that the new software image is being programmed into the switch's flash memory. When LEDs 1 to 8 are all on, the new software image has been programmed successfully into the switch's flash memory.
4	The switch resets automatically.	After the reset completes, the new software image initiates the switch self-test, which comprises various diagnostic routines and subtests. The LEDs display various patterns to indicate that the subtests are in progress.

Note: You may see an incorrect LED display when downloading the image on a mixed, or Hybrid, stack. All the BU (Base Unit) LEDs may turn on or blink on all BPS 2000 units, as if the stack has failed. However, the stack is operational and the upgrade should complete without problems.

Upgrading software

You follow a different procedure depending if you are using a Pure BPS 2000 stack or a Hybrid stack.

The stacking software compatibility requirements are as follows:

- Pure BPS 2000 stack—All units must be running the same software version.
- Pure BayStack 450 stack—All units must be running the same software version.
- Hybrid stack:
  - All BPS 2000 units must be running the same software version.
  - All BayStack 410 units must be running the same software version.
  - All BayStack 450 units must be running the same software version.
  - All software versions must have the identical ISVN.

This section discusses the following topics:

- "Upgrading software in a Pure BPS 2000 stack or a standalone BPS 2000," next
- "Upgrading software in a Hybrid stack" on page 121

Upgrading software in a Pure BPS 2000 stack or a standalone BPS 2000

To download, or upgrade, software in a Pure BPS 2000 stack or a standalone BPS 2000 unit:

1 From the main menu, choose Configuration > Software Download.

The Software Download page opens (Figure 45).

2 In the BPS 2000 Image Filename field, enter the image file name.

3 In the TFTP Server IP Address, enter the IP address of your TFTP load host.

4 Choose BPS 2000 Image in the Start TFTP Load of New Image field.

5 Click Submit.

The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

6 From the main menu, choose Configuration > Software Download.

7 In the BPS 2000 Diagnostics Filename field, enter the name of the BPS 2000 diags file.

8 In the TFTP Server IP Address, enter the IP address of your TFTP load host.

9 In the Start TFTP Load of New Image field, choose BPS 2000 Diagnostics.

10 Click Submit.

The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

However, if you are currently using software version 1.0, 1.0.1, or 1.1, you must upgrade to software version 1.1.1 before upgrading to version 2.0.

Upgrading software in a Hybrid stack

The physical order of the units and the unit numbering in the Hybrid stack does not affect the upgrading process at all. In addition, the cabling order regarding upstream/downstream neighbors does not affect the process.

Before you attempt to download new software (or upgrade software) to a Hybrid (mixed) stack, you *must* ensure that the Interoperability Software Version Numbers (ISVN) are identical. That is, the ISVN number for the BayStack 450 switch and BayStack 410 switch must have the same ISVN as the BPS 2000. If the ISVNs are not the same, the stack does not operate. The ISVNs and the accompanying software release are:

- ISVN 1
    - BayStack 410 or Bay Stack 450—version 3.1
    - BPS 2000—versions 1.0 and 1.0.1
- ISVN 2
    - BayStack 410 or BayStack 450—versions 4.0 and 4.1
    - BPS 2000—versions 1.1, 1.1.1, 1.2, and 2.0

This section describe the steps for the following software upgrades:

- "Upgrading software when ISVN is 2," next
- "Upgrading software when ISVN is 1" on page 122

Upgrading software when ISVN is 2

If you are currently using BPS 2000 software version 1.0, 1.0.1, or 1.1, you must upgrade to software version 1.1.1 before upgrading to BPS 2000 version 2.0.

To upgrade a Hybrid stack to BPS 2000 software version 2.0 when the ISVN numbers of the units are 2:

1. Choose Configuration > Software Download from the main menu.

   The Software Download screen appears (Figure 46).

2. In the BPS 2000 Image Filename field, enter the name of the BPS 2000 image file.

3 In the TFTP Server IP Address, enter the IP address of your TFTP load host.

4 In the Start TFTP Load of New Image field, choose BPS 2000 Image in the Start TFTP Load of New Image field.

5 Click Submit.

The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

6 From the main menu, choose Configuration > Software Download.

7 In the BPS 2000 Diagnostics Filename field, enter the name of the BPS 2000 diags file.

8 In the TFTP Server IP Address, enter the IP address of your TFTP load host.

9 In the Start TFTP Load of New Image field, choose BPS 2000 Diagnostics.

10 Click Submit.

The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

11 From the main menu, choose Configuration > Software Download.

Refer to the documentation for the BayStack 450 and BayStack 410 switches to upgrade the software on those switches.

Upgrading software when ISVN is 1

To upgrade a Hybrid stack to BPS 2000 software version 2.0 when the ISVN numbers of the units are 1:

1 Choose Configuration > Software Download from the main menu.

The Software Download screen appears (Figure 46).

2 In the BPS 2000 Image Filename field, enter the name of the BPS 2000 image file.

3 In the 450 Image Filename field, enter the name of the BayStack 450/410 image file.

4 In the TFTP Server IP Address, enter the IP address of your TFTP load host.

5. In the Start TFTP Load of New Image field, choose Both BPS 2000 and 450 Image.

Note: If you do not download both the BPS 2000 and BayStack 410/450 images simultaneously, the stack may not form.

---

6. Click Submit.

   The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

7. From the main menu, choose Configuration > Software Download.
8. In the 450 Image Filename field, enter the name of the other 450 image file.
9. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
10. In the Start TFTP Load of New Image field, choose 450 Image.
11. Click Submit.

    The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

12. From the main menu, choose Configuration > Software Download.
13. In the BPS 2000 Diagnostics Filename field, enter the name of the BPS 2000 diags file.
14. In the TFTP Server IP Address, enter the IP address of your TFTP load host.
15. In the Start TFTP Load of New Image field, choose BPS 2000 Diagnostics.
16. Click Submit.

    The system resets, which may take a few minutes. The system opens to the System Information page (Figure 4).

17. From the main menu, choose Configuration > System.

    The System page opens (Figure 19).

18. Validate that the ISVN on both the BPS 2000 and the BayStack are 2.

Refer to *Using the Business Policy Switch 2000 Software Version 2.0* for further information on downloading software and upgrading software in standalone BPS 2000 units, in pure BPS 2000 stacks, and in mixed (Hybrid) stacks.

Storing and retrieving a switch configuration file from a TFTP server

You can store switch and stack configuration parameters on a Trivial File Transfer Protocol (TFTP) server. You can retrieve the configuration parameters of a standalone switch or an entire stack and use the retrieved parameters to automatically configure a replacement switch or stack.

To store a switch or stack configuration, you must set up the file on your TFTP server and set the filename read/write permission to enabled.

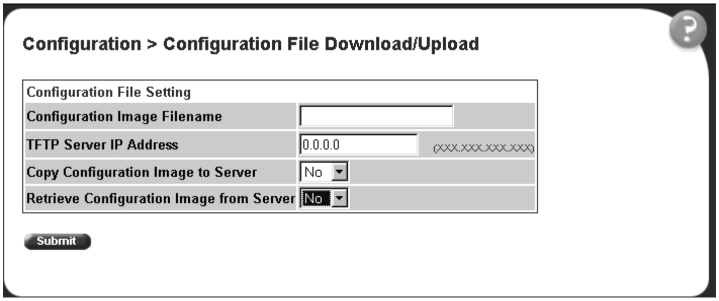
To download the BPS 2000 configuration file, a properly configured TFTP server must be present in your network, and the policy switch must have an IP address. To learn how to configure the switch or stack IP address, refer to "Configuring BootP, IP, and gateway settings" on page 64.

To store or retrieve a switch or stack configuration file:

1 From the main menu, choose Configuration > Configuration File.

The Configuration File Download/Upload page opens (Figure 47).

Figure 47 Configuration File Download/Upload page



Configuration > Configuration File Download/Upload

Configuration File Setting		
Configuration Image Filename		
TFTP Server IP Address	0.0.0.0	(XXX.XXX.XXX.XXX)
Copy Configuration Image to Server	No	
Retrieve Configuration Image from Server	No	

Table 39 describes the items on the Configuration File page.

Table 39 Configuration File page items

Item	Range	Description
Configuration Image Filename	1..32	Type the configuration file name.
TFTP Server IP Address	XXX.XXX.XXX.XXX	Type the IP address of the TFTP load host.
Copy Configuration Image to Server	(1) Yes (2) No	Choose whether or not to copy the configuration image to the server.
Retrieve Configuration Image from Server	(1) Yes (2) No	Choose whether or not to retrieve the configuration image from a server. If you choose Yes, the download process begins immediately and, when completed, causes the switch or stack to reset with the new configuration parameters.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Table 40 describes the requirements for storing or retrieving configuration parameters on a TFTP server.

Table 40 Requirements for storing or retrieving configuration parameters on a TFTP server

Requirements
• The Configuration File feature can only be used to copy *standalone switch configuration parameters to other standalone switches* or to copy *stack configuration parameters to other stack configurations*. For example, you cannot duplicate the configuration parameters of a unit in a *stack* configuration and use it to configure a *standalone* switch.
• A configuration file obtained from a standalone switch can only be used to configure other standalone switches that have the same firmware revision and model type as the donor standalone switch.
• A configuration file obtained from a stack unit can only be used to configure other stacks that have the same number of switches, firmware version, model types, and physical IDs as the stack the donor stack unit resides in.
• Reconfigured stacks are configured according to the unit order number of the donor unit. For example, the configuration file parameters from a donor unit with physical ID *x* are used to reconfigure the unit with physical ID *x.*
• The configuration file also duplicates any settings that exist for any MDA that is installed in the donor switch. If you use the configuration file to configure another switch that has the same MDA model installed, the configuration file settings will also apply to and override the existing MDA settings.

Table 41 describes the parameters that are not saved to the configuration file.

Table 41 Parameters not saved to the configuration file

These parameters are not saved:	**Used in this screen:**	**See page:**
In-Band Stack IP Address	IP Configuration/Setup	64
In-Band Switch IP Address		
In-Band Subnet Mask		
Default Gateway		
Configuration Image Filename	Configuration File Download/Upload	124
TFTP Server IP Address		
Console Read-Only Switch Password	Console/Comm Port Configuration	127
Console Read-Write Switch Password		
Console Read-Only Stack Password		
Console Read-Write Stack Password		

Configuring port communication speed

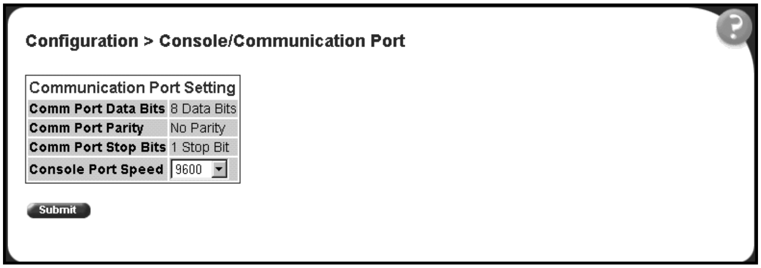
You can view the current console/communication port settings and configure the console port baud rate to match the baud rate of the console terminal.

To view current console/communication port settings and configure console port speed:

1 From the main menu, choose Configuration > Console/Comm Port.

The Console/Communication Port page opens (Figure 48).

Figure 48 Console/Communication Port page



Configuration > Console/Communication Port

Communication Port Setting	
Comm Port Data Bits	8 Data Bits
Comm Port Parity	No Parity
Comm Port Stop Bits	1 Stop Bit
Console Port Speed	9600

Table 42 describes the items on the Console/Communication Port page.

Table 42 Console/Communication Port Setting page items

Item	Range	Description
Comm Port Data Bits		The current console communication port data bit setting.
Comm Port Parity		The current console communication port parity setting.
Comm Port Stop Bits		The current console communication port stop bit setting.
Console Port Speed	2400 4800 9600 19200 38400	Choose the console port speed baud rate. Note: The default setting is 9600.
		Caution: If you choose a baud rate that does not match your console terminal baud rate, you will lose communication with the configuration interface when you click Submit.

2 Select from the list.

3 Click Submit.

Setting system operational modes

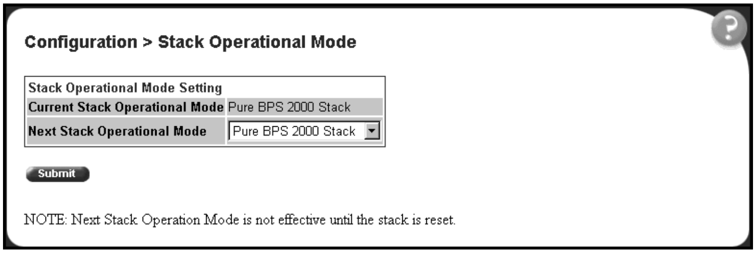
You can set the next stack mode operation of either a stack of BPS 2000 only, or a mixed stack of BPS 2000 and BayStack 450 and 410 switches.

To set the next stack mode operation:

1 From the main menu, choose Configuration > Stack Operational Mode.

The Stack Operational Mode Setting page opens (Figure 49).

Figure 49 Stack Operational Mode page



Configuration > Stack Operational Mode

Stack Operational Mode Setting	
Current Stack Operational Mode	Pure BPS 2000 Stack
Next Stack Operational Mode	Pure BPS 2000 Stack

NOTE: Next Stack Operation Mode is not effective until the stack is reset.

Table 43 describes the items on the Stack Operational Mode Setting page.

Table 43 Stack Operational Mode page items

Item	Range	Description
Current Stack Operational Mode		Current stack operational mode. The options are Pure BPS 2000 Stack or Hybrid Stack.
Next Stack operational Mode	(1) Pure BPS 2000 Stack (2) Hybrid Stack	Choose whether your stack is BPS 2000 only, or a mixed stack of BayStack 450 and BPS 2000 (Hybrid Stack).

2 Select from the list.

3 Click Submit.

Chapter 5
Configuring remote network monitoring (RMON)

The RMON management information base (MIB) is an interface between the RMON agent on a BayStack 450 switch or Business Policy Switch 2000 and RMON management applications such as the Web-based management user interface. It defines objects that are suitable for the management of any type of network. Some groups are specifically targeted for Ethernet networks.

The RMON agent continuously collects statistics and proactively monitors the switch.

This RMON options available to you are:

- "Configuring RMON fault threshold parameters," (next)
- "Viewing the RMON fault event log" on page 133
- "Viewing the system log" on page 134
- "Viewing RMON Ethernet statistics" on page 136
- "Viewing RMON history" on page 140

Note: To access the software version 2.0 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Configuring RMON fault threshold parameters

Alarms are useful when you need to know when the value of some variable goes out of range. RMON alarms can be defined on any MIB variable that resolves to an integer value. String variables (such as system description) cannot be used as alarm variables.

Creating an RMON fault threshold

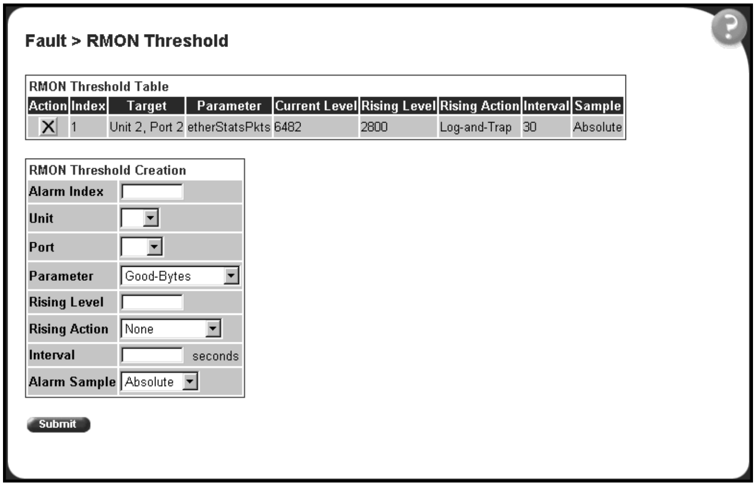
You can create the RMON threshold parameters for fault notification (alarms).

To create an RMON threshold:

1 From the main menu, choose Fault > RMON Threshold.

The RMON Threshold page opens (Figure 50).

Figure 50 RMON Threshold page



Fault > RMON Threshold

RMON Threshold Table

Action	Index	Target	Parameter	Current Level	Rising Level	Rising Action	Interval	Sample
☒	1	Unit 2, Port 2	etherStatsPkts	6482	2800	Log-and-Trap	30	Absolute

RMON Threshold Creation

Alarm Index	
Unit	
Port	
Parameter	Good-Bytes
Rising Level	
Rising Action	None
Interval	seconds
Alarm Sample	Absolute

Table 44 describes the items on the RMON Threshold page.

Table 44 RMON Threshold page items

Item	Range	Description
☒		Deletes the row.
Index/Alarm Index	1..10	Type the unique number to identify the alarm entry.
Target	Integer	The unit number and port number.
Unit	1..8	Choose the switch on which to configure port alarms.
Port	1..28	Choose the port on which to set an alarm.
Parameter	(1) Good-Bytes (2) Good-Packets (3) Multicast (4) Broadcast (5) CRC-Errors (6) Runts (7) Fragments (8) Frame-Too-Long (9) Collisions	Choose the sampled statistic.
Current Level	Integer	The value of the statistic during the last sampling period. Note: If the sample type is Delta, the value is the difference between the samples at the *beginning and end* of the period. If the sample type is Absolute, the value is the sampled value at the *end* of the period.
Rising Level	Integer	Type the event entry to be used when a rising threshold is crossed. Note: When the current sampled value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event will be generated. After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches the Falling Threshold.
Rising Action	(1) None (2) Log (3) SNMP-Trap (4) Log-and-Trap	Choose the type of notification for the event. Selecting Log generates an entry in the RMON Event Log table for each event. Selecting SNMP Trap sends an SNMP trap to one or more management stations.

Table 44 RMON Threshold page items (continued)

Item	Range	Description
Interval		Type the time period (in seconds) to sample data and compare the data to the rising and falling thresholds.
Sample/Alarm Sample	(1) Absolute (2) Delta	Choose the sampling method: Absolute: *Absolute* alarms are defined on the current value of the alarm variable. An example of an alarm defined with absolute value is card operating status. Because this value is not cumulative, but instead represents states, such as card up (value 1) and card down (value 2), you set it for absolute value. Therefore, an alarm could be created with a rising value of 2 and a falling value of 1 to alert a user to whether the card is up or down. Delta: Most alarm variables related to Ethernet traffic are set to *delta* value. Delta alarms are defined based on the difference in the value of the alarm variable between the start of the polling period and the end of the polling period. Delta alarms are sampled twice per polling period. For each sample, the last two values are added together and compared to the threshold values. This process increases precision and allows for the detection of threshold crossings that span the sampling boundary. Therefore, if you keep track of the current values of a given delta-valued alarm and add them together, the result is twice the actual value. (This result is not an error in the software.)

2. In the RMON Threshold Creation section, type information in the text boxes, or select from a list.
3. Click Submit.

   The new configuration is displayed in the RMON Threshold Table (Figure 50).

Note: RMON threshold configurations are not modifiable. They must be deleted and the information recreated.

Deleting an RMON threshold configuration

To delete an existing RMON threshold configuration:

1. From the main menu, choose Fault > RMON Threshold.

   The RMON Threshold page opens (Figure 50).

2. In the RMON Threshold Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the RMON threshold configuration.
   - Click Cancel to return to the RMON Threshold page without making changes.

Viewing the RMON fault event log

RMON events and alarms work together to notify you when values in your network go out of a specified range. When values pass the specified ranges, the alarm is triggered and "fires." The event specifies how the activity is recorded.

An event specifies whether a trap, a log, or a trap and a log are generated to view alarm activity. When RMON is globally enabled, two default events are generated:

- Rising Event
- Falling Event

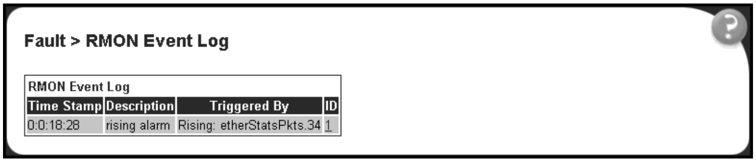
Default events specify that when an alarm goes out of range, the firing of the alarm is tracked in both a trap and a log. For example, when an alarm fires at the rising threshold, the rising event specifies that this information be sent to both a trap and a log. The RMON Event Log page works in conjunction with the RMON Threshold page to enable you to view a history of RMON fault events.

To view a history of RMON fault events:

➨ From the main menu, choose Fault > RMON Event Log.

The RMON Event Log page opens (Figure 51).

Figure 51 RMON Event Log page



Fault > RMON Event Log

RMON Event Log

Time Stamp	Description	Triggered By	ID
0:0:18:28	rising alarm	Rising: etherStatsPkts.34	1

Table 45 describes the fields on the RMON Event Log page.

Table 45 RMON Event Log page fields

Item	Description
Time Stamp	The time the event occurred.
Description	An implementation dependent description of the event that activated this log entry.
Triggered By	A comment describing the source of the event.
ID	The event that generated this log entry.

Viewing the system log

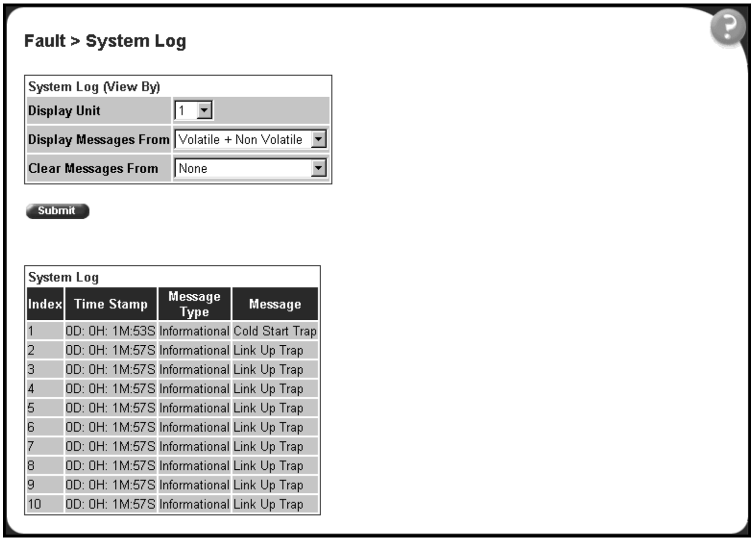
You can view a display of messages contained in non-volatile random access memory (NVRAM) or dynamic random access memory (DRAM) and NVRAM.

To open the System Log page:

1 From the main menu, choose Fault > System Log.

The System Log page opens (Figure 52).

Figure 52 System Log page



System Log (View By)

Display Unit	1
Display Messages From	Volatile + Non Volatile
Clear Messages From	None

System Log

Index	Time Stamp	Message Type	Message
1	0D: 0H: 1M:53S	Informational	Cold Start Trap
2	0D: 0H: 1M:57S	Informational	Link Up Trap
3	0D: 0H: 1M:57S	Informational	Link Up Trap
4	0D: 0H: 1M:57S	Informational	Link Up Trap
5	0D: 0H: 1M:57S	Informational	Link Up Trap
6	0D: 0H: 1M:57S	Informational	Link Up Trap
7	0D: 0H: 1M:57S	Informational	Link Up Trap
8	0D: 0H: 1M:57S	Informational	Link Up Trap
9	0D: 0H: 1M:57S	Informational	Link Up Trap
10	0D: 0H: 1M:57S	Informational	Link Up Trap

Table 46 describes the fields on the System Log page.

Table 46 System Log page fields

Section	Item	Range	Description
System Log (View By)	Display Unit	1..8	Choose the unit on which to display messages or clear messages.
	Display Messages From	(1) Non Volatile (2) Volatile + Non Volatile	Choose to display messages from Non Volatile memory (NVRAM) or Volatile (DRAM) and Non Volatile memory. The default settings is Non Volatile.
	Clear Messages From	(1) Volatile (2) Volatile + Non Volatile (3) None	Choose to clear messages from Volatile memory or Volatile and Non Volatile memory. The default settings is None (do not clear messages)
System Log	Index		The number of the event.
	Time Stamp		The time, in hundredths of a second, between system initialization and the time the log messages entered the system.
	Message Type		The type of message. The options are (1) Critical, (2) Serious, and (3) Informational.
	Message		A character string that identifies the origin of the message and the reason why the message was generated.

2. In the System Log (View By) section do one or more of the following:
   - Choose the number of the unit from which to display messages.
   - Choose where to display messages from.
   - Choose to clear messages from Volatile or Non Volatile memory.
3. Click Submit.

   The results of your request are displayed in the System Log section (Figure 52).

Viewing RMON Ethernet statistics

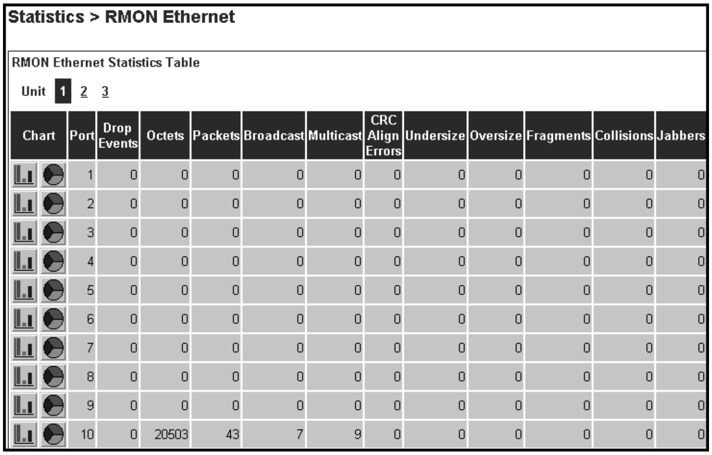
You can gather and graph RMON Ethernet statistics in a variety of formats.

To gather and graph RMON Ethernet statistics:

1 From the main menu, choose Statistics > RMON Ethernet.

The RMON Ethernet page opens (Figure 53).

Figure 53 RMON Ethernet page



Statistics > RMON Ethernet

RMON Ethernet Statistics Table

Unit **1** 2 3

Chart	Port	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors	Undersize	Oversize	Fragments	Collisions	Jabbers
📊 ◕	1	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	2	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	3	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	4	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	5	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	6	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	7	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	8	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	9	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	10	0	20503	43	7	9	0	0	0	0	0	0

Table 47 describes the items on the RMON Ethernet page.

Table 47 RMON Ethernet page items

Item	**Description**
📊	Displays statistics as a bar graph.
◕	Displays statistics as a pie chart.
Port	The port number that corresponds to the selected switch.
Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).

Table 47 RMON Ethernet page items (continued)

Item	**Description**
Packets	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
Broadcast	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
Multicast	The number of good packets received that were directed to the multicast address. This *does not* include packets sent to the broadcast address.
CRC Align Errors	The number of packets received that had a length (excluding and 1518 octets, inclusive, but had either a bad Frame FCS with an integral number of octets (FCS errors) with a non-integral number of octets (alignment error).
Undersize	The number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Oversize	The number of packets received that were longer than 1518 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
Fragments	The number of packets received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Collisions	The “best estimate” number of collisions on this Ethernet segment.
Jabbers	The number of packets received that were longer than 1518 octets in length (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
Packets < = 64 bytes 65-127 bytes 128-255 bytes 256-511 bytes 512-1023 bytes 1024-1518 bytes	The number of octets received (including bad packets) in length (excluding framing bits, but including FCS octets).

2. In the upper-left hand corner, click on the unit number of the device to monitor.
3. Click Submit.

   The RMON Ethernet Statistics Table is updated with information about the selected device (Figure 53).

Viewing RMON Ethernet statistics in a bar graph format

To view RMON Ethernet statistics in a bar graph format:

1. From the main menu, choose Statistics > RMON Ethernet.

   The RMON Ethernet page opens (Figure 53).

2. In the port row of your choice, click the bar graph icon.

   The RMON Ethernet: Chart page appears in a bar graph format (Figure 54).

Figure 54 RMON Ethernet: Chart in a bar graph format

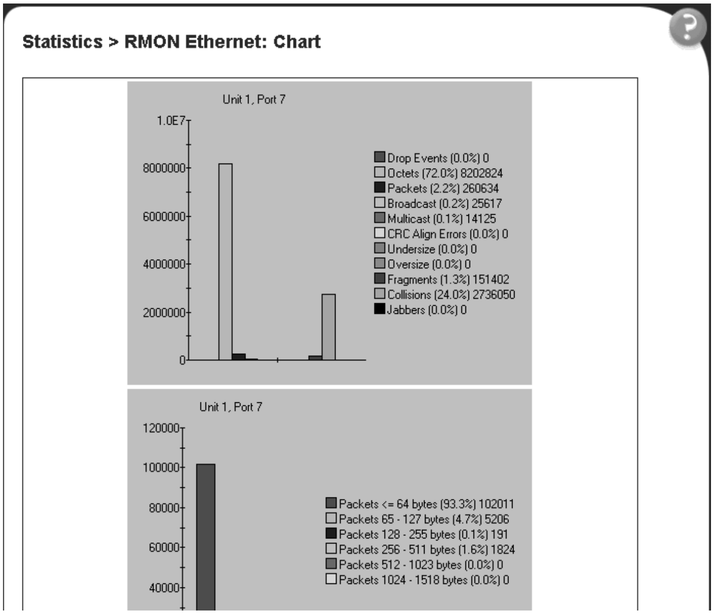

Statistics > RMON Ethernet: Chart
Unit 1, Port 7
1.0E7
8000000
6000000
4000000
2000000
0
Drop Events (0.0%) 0
Octets (72.0%) 8202824
Packets (2.2%) 260634
Broadcast (0.2%) 25617
Multicast (0.1%) 14125
CRC Align Errors (0.0%) 0
Undersize (0.0%) 0
Oversize (0.0%) 0
Fragments (1.3%) 151402
Collisions (24.0%) 2736050
Jabbers (0.0%) 0
Unit 1, Port 7
120000
100000
80000
60000
40000
Packets <= 64 bytes (93.3%) 102011
Packets 65 - 127 bytes (4.7%) 5206
Packets 128 - 255 bytes (0.1%) 191
Packets 256 - 511 bytes (1.6%) 1824
Packets 512 - 1023 bytes (0.0%) 0
Packets 1024 - 1518 bytes (0.0%) 0

   Table 47 describes the items on the RMON Ethernet: Chart page.

3. To refresh statistical information, go to the bottom of the page and click Update, or click Back to return to the Ethernet Statistics page.

Viewing RMON Ethernet statistics in a pie chart format

To view RMON Ethernet statistics in a pie chart format:

1 From the main menu, choose Statistics > RMON Ethernet.

The RMON Ethernet page opens (Figure 53).

2 In the port row of your choice, click the pie chart icon.

The RMON Ethernet: Chart page appears in a pie chart format (Figure 55).

Figure 55 RMON Ethernet: Chart in a pie chart format

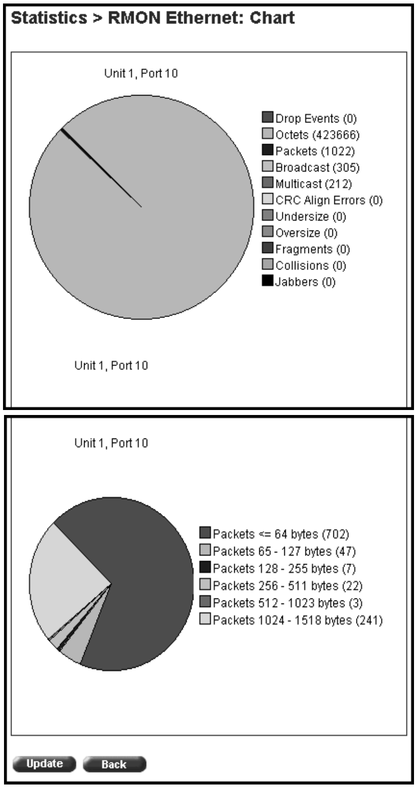

Statistics > RMON Ethernet: Chart
Unit 1, Port 10
Drop Events (0)
Octets (423666)
Packets (1022)
Broadcast (305)
Multicast (212)
CRC Align Errors (0)
Undersize (0)
Oversize (0)
Fragments (0)
Collisions (0)
Jabbers (0)
Unit 1, Port 10
Unit 1, Port 10
Packets <= 64 bytes (702)
Packets 65 - 127 bytes (47)
Packets 128 - 255 bytes (7)
Packets 256 - 511 bytes (22)
Packets 512 - 1023 bytes (3)
Packets 1024 - 1518 bytes (241)
Update
Back

Table 47 describes the items on the RMON Ethernet: Chart page.

3 To refresh statistical information, click Update, or click Back to return to the Ethernet Statistics page.

Viewing RMON history

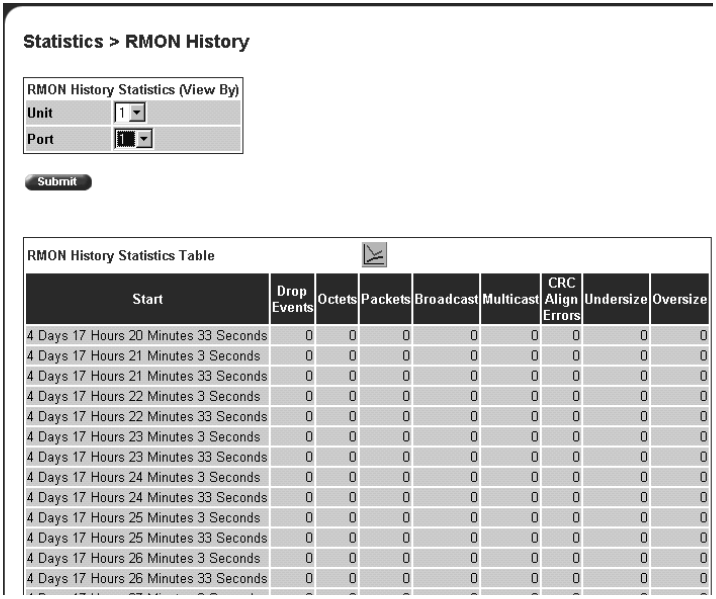
You can view a periodic statistical sampling of data from various types of networks.

To view periodic statistical data:

1 From the main menu, choose Statistics > RMON History.

The RMON History page opens (Figure 56).

Figure 56 RMON History page



Statistics > RMON History

RMON History Statistics (View By)	
Unit	1
Port	1

RMON History Statistics Table

Start	Drop Events	Octets	Packets	Broadcast	Multicast	CRC Align Errors	Undersize	Oversize
4 Days 17 Hours 20 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 21 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 21 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 22 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 22 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 23 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 23 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 24 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 24 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 25 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 25 Minutes 33 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 26 Minutes 3 Seconds	0	0	0	0	0	0	0	0
4 Days 17 Hours 26 Minutes 33 Seconds	0	0	0	0	0	0	0	0

Table 48 describes the items on the RMON History page.

Table 48 RMON History page items

Section	**Item**	**Description**
RMON History Statistics (View By)	Unit	Choose the unit number to be monitored.
	Port	Choose the port number to be monitored.
	📈	Displays statistics as a line graph.
RMON History Statistics Table	Start	The value of the sysUPTime at the start of the interval over which this sample was measured.
	Drop Events	The number of events in which packets were dropped by the interface due to a lack of resources.
	Octets	The number of octets of data (including those in bad packets) received on the network (excluding framing bits, but including Frame Check Sequence (FCS) octets).
	Packets	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
	Broadcast	The number of good packets received that were directed to the broadcast address. This *does not* include multicast packets.
	Multicast	The number of good packets received that were directed to the multicast address. This *does not* include packets sent to the broadcast address.
	CRC Align Errors	The number of packets received that had a length (excluding and 1518 octets, inclusive, but had either a bad Frame FCS with an integral number of octets (FCS errors) with a non-integral number of octets (alignment error).
	Undersize	The number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.
	Oversize	The number of packets received that were longer than 1518 octets long (excluding framing bits, but including FCS octets) and were otherwise well-formed.

2 In the RMON History Statistics section, choose the unit and port number to be monitored.

3 Click Submit.

The RMON History Statistics Table is updated with information about the selected device and port (Figure 56).

Viewing RMON statistics in a line graph format

You can view RMON statistical data in a line graph format.

To view statistics in a line graph format:

1. From the main menu, choose Statistics > RMON History.

   The RMON History page opens (Figure 56).

2. In the RMON History Statistics Table, click the line graph icon.
3. Click Back to return to the RMON History page.

Chapter 6
Viewing system statistics

The options available to monitor system statistical data are:

- "Viewing port statistics," (next)
- "Viewing all port errors" on page 148
- "Viewing interface statistics" on page 150
- "Viewing Ethernet error statistics" on page 153
- "Viewing transparent bridging statistics" on page 157

Note: To access the software version 2.0 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Viewing port statistics

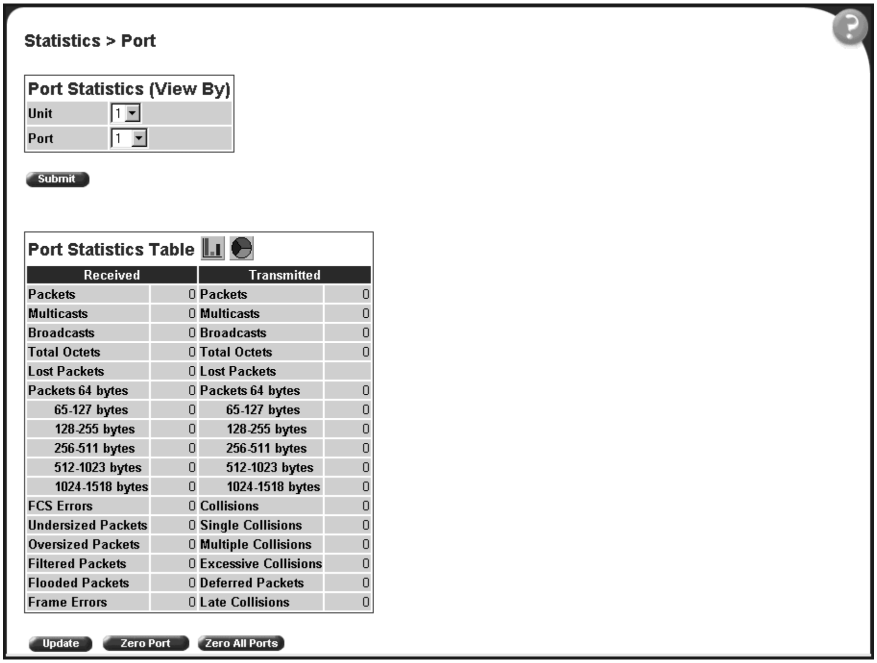
You can view detailed statistics about a selected switch port in a stacked or standalone configuration. Both received and transmitted statistics are displayed so that you can compare throughput or other port parameters.

To view statistical data about a selected switch port:

1. From the main menu, choose Statistics > Port.

   The Port page opens (Figure 57).

Figure 57 Port page



Statistics > Port

Port Statistics (View By)

Unit: 1

Port: 1

Port Statistics Table 📊 ◔

Received		Transmitted	
Packets	0	Packets	0
Multicasts	0	Multicasts	0
Broadcasts	0	Broadcasts	0
Total Octets	0	Total Octets	0
Lost Packets	0	Lost Packets	
Packets 64 bytes	0	Packets 64 bytes	0
65-127 bytes	0	65-127 bytes	0
128-255 bytes	0	128-255 bytes	0
256-511 bytes	0	256-511 bytes	0
512-1023 bytes	0	512-1023 bytes	0
1024-1518 bytes	0	1024-1518 bytes	0
FCS Errors	0	Collisions	0
Undersized Packets	0	Single Collisions	0
Oversized Packets	0	Multiple Collisions	0
Filtered Packets	0	Excessive Collisions	0
Flooded Packets	0	Deferred Packets	0
Frame Errors	0	Late Collisions	0

Table 49 describes the items on the Port page.

Table 49 Port page items

Section	Item	Description
Port Statistics (View By)	Unit	Choose the number of the switch to monitor.
	Port	Choose the switch's port number to monitor.
	📊	Displays statistics in a bar graph format.
	◔	Displays statistics in a pie chart format.

Table 49 Port page items (continued)

Section	Item	Description
Port Statistics Table	Packets	The number of packets received/transmitted on this port, including bad packets, broadcast packets, and multicast packets.
	Multicast	The number of good multicast packets received/transmitted on this port, excluding broadcast packets.
	Broadcasts	The number of good broadcast packets received/transmitted on this port.
	Total Octets	The number of octets of data received/transmitted on this port, including data in bad packets and FCS octets, and framing bits.
	Lost Packets	The number of packets discarded on this port when the capacity of the port transmit buffer was exceeded.
	Packets = 64 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 65-127 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 128-255 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 256-511 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 512-1023 bytes	The number of packets this size received/transmitted successfully on this port.
	Packets 1024-1518 bytes	The number of packets this size received/transmitted successfully on this port.
	FCS Errors	The number of valid-size packets received on this port with proper framing but discarded because of cyclic redundancy check (CRC) errors.
	Undersized Packets	The number of packets received on this port with fewer than 64 bytes and with proper CRC and framing (also known as short frames or runts).
	Oversized Packets	The number of packets that were received on this port with proper CRC and framing that meet the following requirements: • 1518 bytes if no VLAN tag exists • 1522 bytes if a VLAN tag exists
	Filtered Packets	The number of packets filtered, but not forwarded on this port.
	Flooded Packets	The number of packets flooded (forwarded) through this port because the destination address was not recognized in the address database.
	Frame Errors	The number of valid-size packets received on this port but discarded because of CRC errors and improper framing.

Table 49 Port page items (continued)

Section	Item	Description
Port Statistics Table, cont.	Collisions	The number of collisions detected on this port.
	Single Collisions	The number of packets that were transmitted successfully on this port after a single collision.
	Multiple Collisions	The number of packets that were transmitted successfully on this port after more than one collision.
	Excessive Collisions	The number of packets lost on this port due to excessive collisions.
	Deferred Packets	The number of frames that were delayed on the first transmission attempt, but never incurred a collision.
	Late Collisions	The number of packets collisions that occurred after a total length of time that exceeded 512 bit-times of packet transmission.

2 In the Port Statistics section, choose the unit number and its port number.

3 Click Submit.

The Port Statistics Table is updated with information about the selected device and port (Figure 57).

4 To update the statistical information, click Update.

Zeroing ports

To clear the statistical information for the currently displayed port:

➨ Click Zero Port.

To clear the statistical information for all ports in a switch or stack configuration:

➨ Click Zero All Ports.

Viewing port statistics in a pie chart format

You can view port statistics in a pie chart format.

To view the displayed statistical information in a pie chart format:

1 In the Port Statistics Table, click the pie chart icon.

The Port: Chart page opens in a pie chart format (Figure 58).

Figure 58 Port: Chart page in a pie chart format

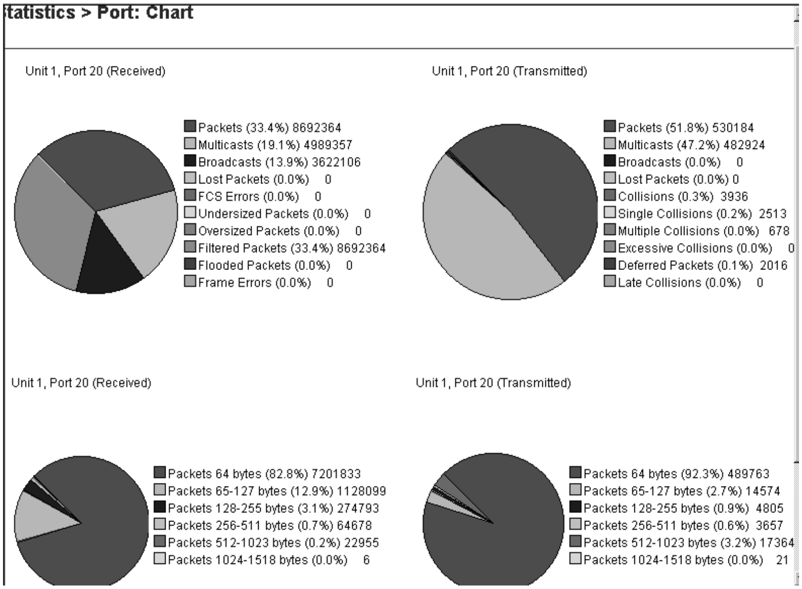

tatistics > Port: Chart
Unit 1, Port 20 (Received)
■ Packets (33.4%) 8692364
■ Multicasts (19.1%) 4989357
■ Broadcasts (13.9%) 3622106
■ Lost Packets (0.0%) 0
■ FCS Errors (0.0%) 0
☐ Undersized Packets (0.0%) 0
■ Oversized Packets (0.0%) 0
■ Filtered Packets (33.4%) 8692364
■ Flooded Packets (0.0%) 0
■ Frame Errors (0.0%) 0
Unit 1, Port 20 (Transmitted)
■ Packets (51.8%) 530184
■ Multicasts (47.2%) 482924
■ Broadcasts (0.0%) 0
■ Lost Packets (0.0%) 0
■ Collisions (0.3%) 3936
☐ Single Collisions (0.2%) 2513
■ Multiple Collisions (0.0%) 678
■ Excessive Collisions (0.0%) 0
■ Deferred Packets (0.1%) 2016
■ Late Collisions (0.0%) 0
Unit 1, Port 20 (Received)
■ Packets 64 bytes (82.8%) 7201833
■ Packets 65-127 bytes (12.9%) 1128099
■ Packets 128-255 bytes (3.1%) 274793
■ Packets 256-511 bytes (0.7%) 64678
■ Packets 512-1023 bytes (0.2%) 22955
☐ Packets 1024-1518 bytes (0.0%) 6
Unit 1, Port 20 (Transmitted)
■ Packets 64 bytes (92.3%) 489763
■ Packets 65-127 bytes (2.7%) 14574
■ Packets 128-255 bytes (0.9%) 4805
■ Packets 256-511 bytes (0.6%) 3657
■ Packets 512-1023 bytes (3.2%) 17364
☐ Packets 1024-1518 bytes (0.0%) 21

Table 49 describes the items on the Port: Chart page.

2 Click Back to return to the Port page.

Viewing port statistics in a bar graph format

You can view port statistics in a bar graph format.

To view the displayed statistical information in a bar graph format:

1 In the Port Statistics Table, click the bar graph icon.

The Port: Chart page opens in a bar graph format (Figure 59).

Figure 59 Port: Chart page in a bar graph format

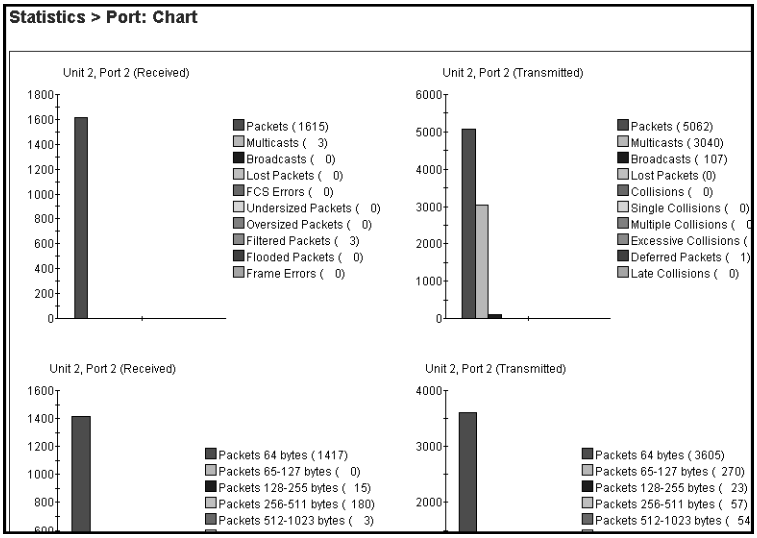

Statistics > Port: Chart
Unit 2, Port 2 (Received)
1800
1600
1400
1200
1000
800
600
400
200
0
Packets (1615)
Multicasts (3)
Broadcasts (0)
Lost Packets (0)
FCS Errors (0)
Undersized Packets (0)
Oversized Packets (0)
Filtered Packets (3)
Flooded Packets (0)
Frame Errors (0)
Unit 2, Port 2 (Transmitted)
6000
5000
4000
3000
2000
1000
0
Packets (5062)
Multicasts (3040)
Broadcasts (107)
Lost Packets (0)
Collisions (0)
Single Collisions (0)
Multiple Collisions (
Excessive Collisions (
Deferred Packets (1)
Late Collisions (0)
Unit 2, Port 2 (Received)
1600
1400
1200
1000
800
Packets 64 bytes (1417)
Packets 65-127 bytes (0)
Packets 128-255 bytes (15)
Packets 256-511 bytes (180)
Packets 512-1023 bytes (3)
Unit 2, Port 2 (Transmitted)
4000
3000
2000
Packets 64 bytes (3605)
Packets 65-127 bytes (270)
Packets 128-255 bytes (23)
Packets 256-511 bytes (57)
Packets 512-1023 bytes (54

Table 49 describes the items on the Port: Chart page.

2 Click Back to return to the Port page.

Viewing all port errors

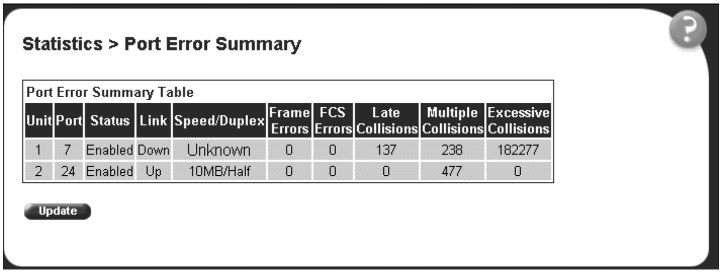
Beginning with software version 1.1, you can view all ports in the entire stack that have an error. If a particular port has no errors, it will not be displayed.

To view a summary of the port errors for the BPS 2000:

1 From the main menu, choose Statistics > Port Error Summary.

The Port Error Summary page opens (Figure 60).

Figure 60 Port Error Summary page



Port Error Summary Table

Unit	Port	Status	Link	Speed/Duplex	Frame Errors	FCS Errors	Late Collisions	Multiple Collisions	Excessive Collisions
1	7	Enabled	Down	Unknown	0	0	137	238	182277
2	24	Enabled	Up	10MB/Half	0	0	0	477	0

Table 50 describes the read-only information displayed in the Port Error Summary Table.

Table 50 Port Error Summary Table fields

Item	Description
Unit	Displays the unit number in the stack.
Port	Displays the port number of the unit.
Status	Displays the status of the port (Enabled/Disabled).
Link	Displays the link status of the port (Up/Down).
Speed/Duplex	Displays the speed at which the port is operating, as well as whether it is in half- or full-duplex mode.
Frame Errors	Displays the number of frame errors received on this port.
FCS Errors	Displays the number of frame check sequence (FCS) errors received on this port.
Late Collisions	Displays the number of late collisions errors received on this port.
Multiple Collisions	Displays the number of multiple collisions errors received on this port.
Excessive Collisions	Displays the number of excessive collisions errors received on this port.

2 To view the latest port statistics, click the Update button at the bottom of the page.

Viewing interface statistics

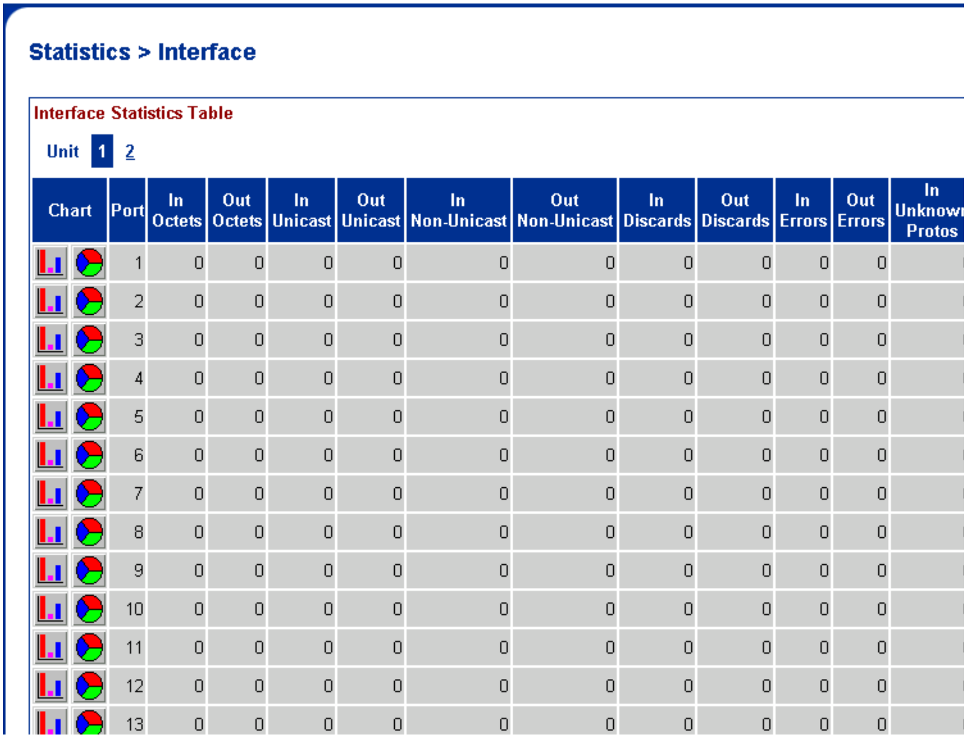
You can view selected switch interface statistics.

To view an interface's statistical information:

1 From the main menu, choose Statistics > Interface.

The Interface page opens (Figure 61).

Figure 61 Interface page



Statistics > Interface

Interface Statistics Table

Unit **1** 2

Chart	Port	In Octets	Out Octets	In Unicast	Out Unicast	In Non-Unicast	Out Non-Unicast	In Discards	Out Discards	In Errors	Out Errors	In Unknow Protos
	1	0	0	0	0	0	0	0	0	0	0	
	2	0	0	0	0	0	0	0	0	0	0	
	3	0	0	0	0	0	0	0	0	0	0	
	4	0	0	0	0	0	0	0	0	0	0	
	5	0	0	0	0	0	0	0	0	0	0	
	6	0	0	0	0	0	0	0	0	0	0	
	7	0	0	0	0	0	0	0	0	0	0	
	8	0	0	0	0	0	0	0	0	0	0	
	9	0	0	0	0	0	0	0	0	0	0	
	10	0	0	0	0	0	0	0	0	0	0	
	11	0	0	0	0	0	0	0	0	0	0	
	12	0	0	0	0	0	0	0	0	0	0	
	13	0	0	0	0	0	0	0	0	0	0	

Table 51 describes the items on the Interface page.

Table 51 Interface page items

Item	Description
📊	Displays statistics in a bar graph format.
◕	Displays statistics in a pie chart format.
Port	The port number corresponding to the selected switch.
In Octets	The number of octets received on the interface, including framing characters.
Out Octets	The number of octets transmitted out of the interface, including framing characters.
In Unicast	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Out Unicast	The number of packets that higher-layer protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
In Non-Unicast	The number of non-unicast packets, for example, subnetwork-broadcast or subnetwork-multicast packets, delivered to a higher protocol.
Out Non-Unicast	The number of packets that higher-level protocols requested be transmitted to a non-unicast address. For example, a subnetwork-broadcast or a subnetwork multicast address, including those that were discarded or not sent.
In Discards	The number of inbound packets which were selected to be discarded even though no errors were detected to prevent their being delivered to a higher-layer protocol. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
Out Discards	The number of outbound packets which were selected to be discarded even though no errors were detected to prevent their being transmitted. Packet discarding is not arbitrary. One reason for discarding packets is to free buffer space.
In Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Out Errors	The number of outbound packets that could not be transmitted because of errors.
In Unknown Protos	The number of packets received through the interface that were discarded because of an unknown or unsupported protocol.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

The page is updated with the information for the selected device (Figure 61).

3 To update the statistical information, click Update.

Viewing interface statistics in a pie chart format

You can view interface statistics in a pie chart format.

To view interface statistics in a pie chart format:

1. From the main menu, choose Statistics > Interface.

   The Interface page opens (Figure 61).

2. In the port row of your choice, click the pie chart icon.

   The Interface: Chart page opens in a pie chart format (Figure 62).

Figure 62 Interface: Chart in a pie chart format

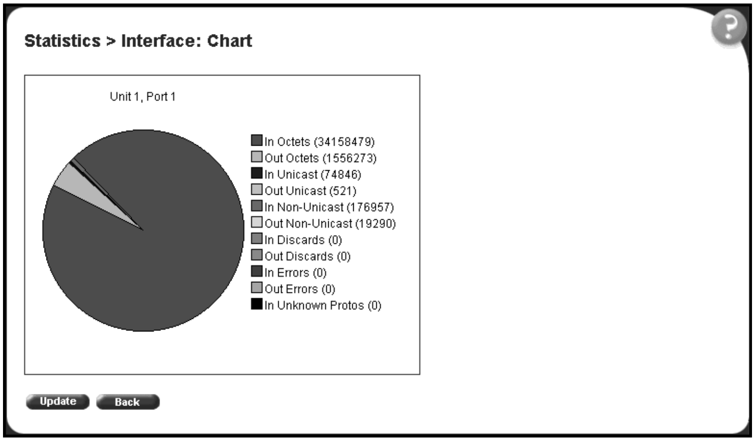

Statistics > Interface: Chart
Unit 1, Port 1
In Octets (34158479)
Out Octets (1556273)
In Unicast (74846)
Out Unicast (521)
In Non-Unicast (176957)
Out Non-Unicast (19290)
In Discards (0)
Out Discards (0)
In Errors (0)
Out Errors (0)
In Unknown Protos (0)
Update
Back

   Table 51 describes the items on the Interface: Chart page.

3. To update the statistical information, click Update, or click Back to return to the Interface page.

Viewing interface statistics in a bar graph format

You can view interface statistics in a bar graph format.

To view interface statistics in a bar graph format:

1. From the main menu, choose Statistics > Interface.

The Interface page opens (Figure 61).

2 In the port row of your choice, click the bar graph icon.

The Interface: Chart page opens in a bar graph format (Figure 62).

Figure 63 Interface: Chart in a bar graph format

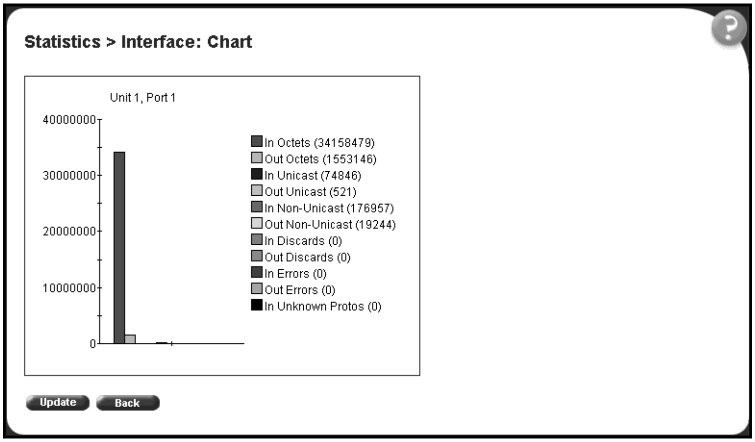

Statistics > Interface: Chart
Unit 1, Port 1
40000000
30000000
20000000
10000000
0
In Octets (34158479)
Out Octets (1553146)
In Unicast (74846)
Out Unicast (521)
In Non-Unicast (176957)
Out Non-Unicast (19244)
In Discards (0)
Out Discards (0)
In Errors (0)
Out Errors (0)
In Unknown Protos (0)
Update
Back

Table 51 describes the items on the Interface: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Interface page.

Viewing Ethernet error statistics

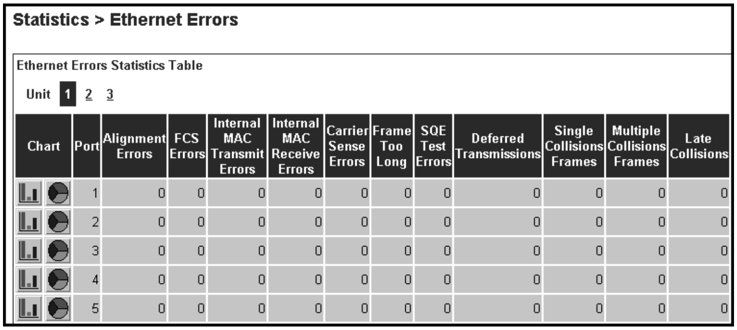
You can view Ethernet error statistics for each monitored interface linked to the Business Policy Switch 2000.

To view Ethernet error statistics:

1 From the main menu, choose Statistics > Ethernet Errors.

The Ethernet Errors page opens (Figure 64).

Figure 64 Ethernet Errors page



Statistics > Ethernet Errors

Ethernet Errors Statistics Table

Unit **1** 2 3

Chart	Port	Alignment Errors	FCS Errors	Internal MAC Transmit Errors	Internal MAC Receive Errors	Carrier Sense Errors	Frame Too Long	SQE Test Errors	Deferred Transmissions	Single Collisions Frames	Multiple Collisions Frames	Late Collisions
📊 ◕	1	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	2	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	3	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	4	0	0	0	0	0	0	0	0	0	0	0
📊 ◕	5	0	0	0	0	0	0	0	0	0	0	0

Table 52 describes the items on the Ethernet Errors page.

Table 52 Ethernet Errors page items

Item	Description
📊	Displays statistics in a bar graph format.
◕	Displays statistics in a pie chart format.
Port	The port number corresponding to the selected switch.
Alignment Errors	The number of frames received on a particular interface that are not an integral number of octets in length and do not pass the FCS check.
FCS Errors	The number of frames received on a particular interface that are an integral number of octets in length, but do not pass the FCS check.
Internal MAC Transmit Errors	The number of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
Internal MAC Receive Errors	The number of frames for which reception on a particular interface fails due to an internal MAC sublayer transmit error. A frame only is counted by an instance of this object if it is not counted by the corresponding instance of either the dot3StatsLateCollisions object, the dot3StatsExcessiveCollisions object, or the dot3StatsCarrierSenseErrors object.
Carrier Sense Errors	The number of times that the carrier sense conditions was lost or never asserted when attempting to transmit a frame on a particular interface.
Frame Too Long	The number of frames received on a particular interface that exceed the maximum permitted frame size.

Table 52 Ethernet Errors page items (continued)

Item	Description
SQE Test Errors	The number of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985, and its generation is described in section 7.2.4.6 of the same document.
Deferred Transmissions	The number of frames for which the first transmission attempt on a particular interface is delayed because the medium is busy.
Single Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.
Multiple Collision Frames	The number of successfully transmitted frames on a particular interface for which transmission is inhibited by a single collision.
Late Collisions	The number of times a collision is detected on a particular interface later than 512 bit-times into the transmission of a packet.
Excessive Collisions	The number of frames for which transmission on a particular interface fails due to excessive collisions.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

The table is updated with the information for the selected device.

3 To refresh the statistical information, click Update.

Viewing Ethernet error statistics in a pie chart format

You can view Ethernet Errors statistics in a pie chart format.

To view Ethernet Errors statistics in a pie chart format:

1 From the main menu, choose Statistics > Ethernet Errors.

The Ethernet Errors page opens (Figure 61).

2 In the port row of your choice, click the pie chart icon.

The Ethernet Errors: Chart page opens in a pie chart format (Figure 65).

Figure 65 Ethernet Error: Chart in a pie chart format

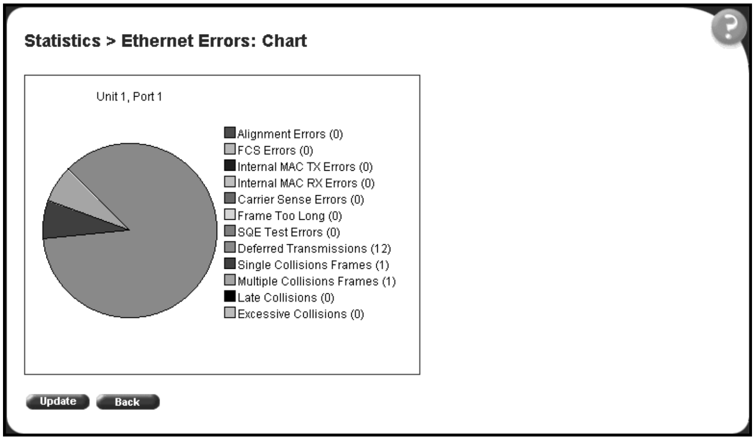

Statistics > Ethernet Errors: Chart
Unit 1, Port 1
Alignment Errors (0)
FCS Errors (0)
Internal MAC TX Errors (0)
Internal MAC RX Errors (0)
Carrier Sense Errors (0)
Frame Too Long (0)
SQE Test Errors (0)
Deferred Transmissions (12)
Single Collisions Frames (1)
Multiple Collisions Frames (1)
Late Collisions (0)
Excessive Collisions (0)
Update
Back

Table 53 describes the items on the Ethernet Errors: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Ethernet Errors page.

Viewing Ethernet error statistics in a bar graph format

You can view Ethernet Errors statistics in a bar graph format.

To view Ethernet errors statistics in a bar graph format:

1 From the main menu, choose Statistics > Ethernet Errors.

The Ethernet Errors page opens (Figure 61).

2 In the port row of your choice, click the bar graph icon.

The Ethernet Errors: Chart page opens in a bar graph format (Figure 66).

Figure 66 Ethernet Error: Chart in a bar graph format

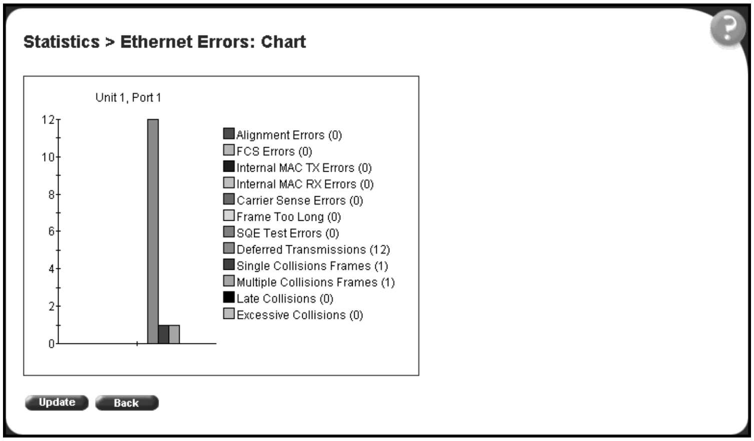

Statistics > Ethernet Errors: Chart
Unit 1, Port 1
12
10
8
6
4
2
0
Alignment Errors (0)
FCS Errors (0)
Internal MAC TX Errors (0)
Internal MAC RX Errors (0)
Carrier Sense Errors (0)
Frame Too Long (0)
SQE Test Errors (0)
Deferred Transmissions (12)
Single Collisions Frames (1)
Multiple Collisions Frames (1)
Late Collisions (0)
Excessive Collisions (0)
Update
Back

Table 52 describes the items on the Ethernet Errors: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Ethernet Errors page.

Viewing transparent bridging statistics

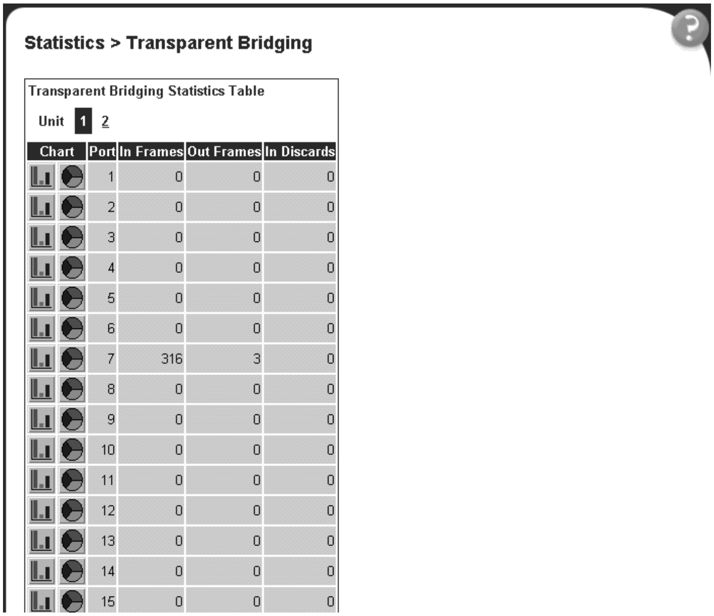
You can view the transparent bridging statistics measured for each monitored interface on the device.

To view transparent bridging statistics:

1 From the main menu, choose Statistics > Transparent Bridging.

The Transparent Bridging page opens (Figure 67).

Figure 67 Transparent Bridging page



Statistics > Transparent Bridging

Transparent Bridging Statistics Table

Unit **1** 2

Chart	Port	In Frames	Out Frames	In Discards
📊 ◕	1	0	0	0
📊 ◕	2	0	0	0
📊 ◕	3	0	0	0
📊 ◕	4	0	0	0
📊 ◕	5	0	0	0
📊 ◕	6	0	0	0
📊 ◕	7	316	3	0
📊 ◕	8	0	0	0
📊 ◕	9	0	0	0
📊 ◕	10	0	0	0
📊 ◕	11	0	0	0
📊 ◕	12	0	0	0
📊 ◕	13	0	0	0
📊 ◕	14	0	0	0
📊 ◕	15	0	0	0

Table 53 describes the items on the Transparent Bridging page.

Table 53 Transparent Bridging page items

Item	Description
📊	Displays statistics in a bar graph format.
◕	Displays statistics in a pie chart format.
Port	The port number that corresponds to the selected switch.
In Frames (dot1dTpPortInFrames)	The number of frames that have been received by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
Out Frames (dot1dTpPortOutFrames)	The number of frames that have been transmitted by this port from its segment. A frame received on the interface corresponding to this port is counted only if it is for a protocol being processed by the local bridging function, including bridge management errors.
In Discards (dot1dTpPortInDiscards)	The number of valid frames received which were discarded by the forwarding process.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

The page is updated with statistics about the selected device and its corresponding port number.

3 To refresh the statistical information, click Update.

Viewing transparent bridging statistics in a pie chart format

You can view measured transparent bridging statistics in a pie chart format.

To view transparent bridging statistics in a pie chart format:

1 From the main menu, choose Statistics > Transparent Bridging.

The Transparent Bridging page opens (Figure 61).

2 In the port row of your choice, click the pie chart icon.

The Transparent Bridging: Chart page opens in a pie chart format (Figure 68).

Figure 68 Transparent Bridging: Chart in a pie chart format

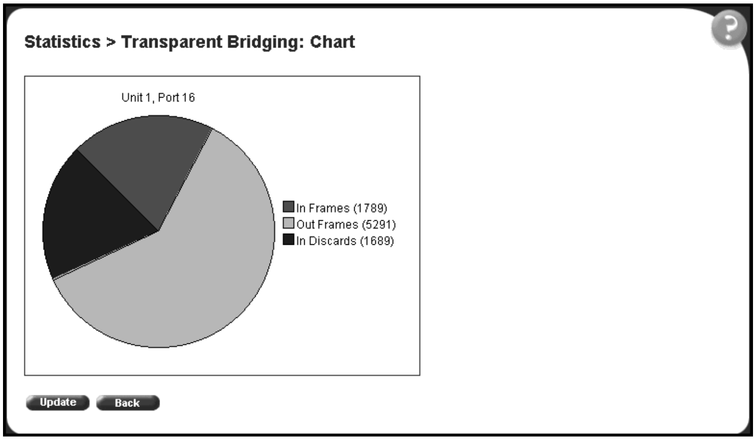


Table 53 describes the items on the Transparent Bridging: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Transparent Bridging page.

Viewing transparent bridging statistics in a bar graph format

You can view measured transparent bridging statistics in a bar graph format.

To view transparent bridging statistics in a bar graph format:

1 From the main menu, choose Statistics > Transparent Bridging.

The Transparent Bridging page opens (Figure 61).

2 In the port row of your choice, click the bar graph icon.

The Transparent Bridging: Chart page opens in a bar graph format (Figure 69).

Figure 69 Transparent Bridging: Chart in a bar graph format

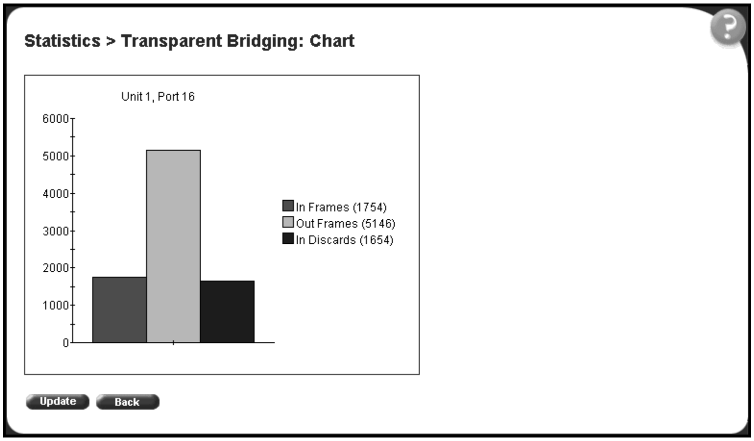

Statistics > Transparent Bridging: Chart
Unit 1, Port 16
6000
5000
4000
3000
2000
1000
0
▨ In Frames (1754)
▨ Out Frames (5146)
▨ In Discards (1654)
Update
Back

Table 53 describes the items on the Transparent Bridging: Chart page.

3 To update the statistical information, click Update, or click Back to return to the Transparent Bridging page.

Chapter 7
Configuring application settings

The options available to configure application settings are:

- "Configuring port mirroring," (next)
- "Configuring rate limiting" on page 165
- "Configuring IGMP" on page 167
- "Viewing Multicast group membership configurations" on page 169
- "Creating and managing virtual LANs (VLANs)" on page 171
- "Configuring VLANs" on page 173
- "Configuring broadcast domains" on page 188
- "Viewing VLAN port information" on page 190
- "Managing spanning tree groups" on page 192
- "Configuring ports for spanning tree" on page 197
- "Changing spanning tree bridge switch settings" on page 199
- "Configuring MultiLink Trunk (MLT) members" on page 202
- "Monitoring MLT traffic" on page 205

Note: To access the software version 2.0 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

Configuring port mirroring

The BPS 2000 supports port mirroring to analyze traffic. You can view existing port mirroring activity and you can configure a specific switch port to mirror up to two specified ports or two MAC addresses. When you configure port mirroring, you have the option to specify either port-based monitoring or address-based monitoring. Refer to *Using the Business Policy Switch 2000 Software Version 2.0* for configuration guidelines for port-mirroring.

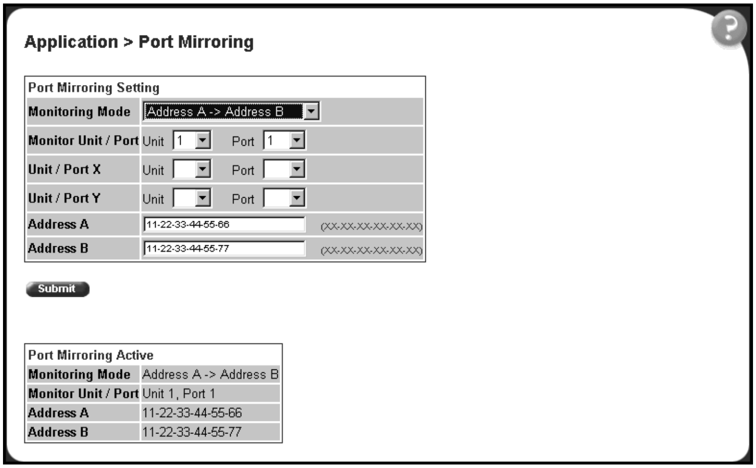
In a stack configuration, you can monitor ports that reside on different units within the stack. For more information, see *Using the Business Policy Switch 2000 Software Version 2.0.*

To configure port mirroring:

1 From the main menu, choose Application > Port Mirroring.

The Port Mirroring page opens (Figure 70).

Figure 70 Port Mirroring page



Port Mirroring Setting

Monitoring Mode	Address A -> Address B	
Monitor Unit / Port	Unit 1	Port 1
Unit / Port X	Unit	Port
Unit / Port Y	Unit	Port
Address A	11-22-33-44-55-66	(XX-XX-XX-XX-XX-XX)
Address B	11-22-33-44-55-77	(XX-XX-XX-XX-XX-XX)

Port Mirroring Active

Monitoring Mode	Address A -> Address B
Monitor Unit / Port	Unit 1, Port 1
Address A	11-22-33-44-55-66
Address B	11-22-33-44-55-77

Note: The Port Mirroring Active section of this only displays those port mirroring configurations you set. If you set no port mirroring configurations, the area will not show rows.

Table 54 describes the items on the Port Mirroring page.

Table 54 Port Mirroring page items

Item	Range	Description
Monitoring Mode	(1) Disabled (2) --> Port X (3) Port X --> (4)<-- --> Port X (5) -->Port X or Port Y --> (6) -->Port X and Port Y --> (7) <-- --> Port X and <-- --> Port Y (8) Address A --> any Address (9) any Address --> Address A (10) <-- --> Address A (11) Address A --> Address B (12) Address A <-- --> Address B	Choose any one of the six port-based monitoring modes or any one of the five address-based monitoring modes. For more information on selecting one of the six port-based modes that activates the port X and port Y screen fields, where you can choose up to two ports to monitor, see Table 55 on page 164. For more information on selecting one of the five address-based modes that activates the Address A and Address B screen fields, where you can specify MAC addresses to monitor, see Table 56 on page 164. The default setting is Disabled.
Port-based monitoring		
Monitor Port	1..28	Choose the switch port to designate as the monitor port.
Port X	1..28	Choose the first switch port to be monitored by the designated monitor port. This port is monitored according to the value “X” in the Monitoring Mode field.
Port Y	1..28	Choose the second switch port to be monitored by the designated monitor port. This port is monitored according to the value “Y” in the Monitoring Mode field.
Address-based monitoring		
Address A	XX-XX-XX-XX-XX-XX	Type the MAC address to monitor by the designated monitor port. This address is monitored according to the value “Address A” in the Monitoring Mode field.
Address B	XX-XX-XX-XX-XX-XX	Type the MAC address to monitor by the designated monitor port. This address is monitored according to the value “Address B” in the Monitoring Mode field.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Selecting one of the port-based monitoring modes activates the port X and/or the port Y screen fields, where you can choose up to two ports to monitor.

Table 55 describes the port-based monitoring modes.

Table 55 Port-based monitoring modes

Item	Description
Disabled	Choose this option to disable port-based monitoring. The default setting is Disabled.
--> Port X	Choose this option to monitor all traffic received by port X.
Port X -->	Choose this option to monitor all traffic transmitted by port X.
<-- --> Port X	Choose this option to monitor all traffic received and transmitted by port X.
--> Port X or Port Y -->	Choose this option to monitor all traffic received by port X or transmitted by port Y. Note: Do not use this mode for multicast and broadcast traffic.
--> Port X and Port Y -->	Choose this option to monitor all traffic received by port X (destined to port Y) and then transmitted by port Y (one way conversation steering). Note: Do not use this mode for multicast and broadcast traffic
<-- --> Port X and Port Y <-- -->	Choose this option to monitor all traffic received by port X and then transmitted by port Y or transmitted by port X and received by port Y (two way conversation steering). Note: Do not use this mode for multicast and broadcast traffic

Selecting any one of the address-based monitoring modes activates the Address A and Address B screen fields, where you can specify MAC addresses to monitor.

Table 56 describes the address-based monitoring modes.

Table 56 Address-based monitoring modes

Item	Description
Disabled	Choose this option to disable port-based monitoring. The default setting is Disabled.
Address A --> any Address	Choose this option to monitor all traffic transmitted from Address A to any address.
any Address --> Address A	Choose this option to monitor all traffic received by Address A from any address.
<-- --> Address A	Choose this option to monitor all traffic received by or transmitted by Address A.
Address A --> Address B	Choose this option to monitor all traffic transmitted by Address A that goes to Address (one way conversation steering).
Address A <-- --> Address B	Choose this option to monitor all traffic received by Address A and then transmitted by Address B or transmitted by Address A and received by Address B (two way conversation steering).

Configuring rate limiting

You can view the current forwarding rate of broadcast and/or multicast packets, and configure the BPS 2000 to limit the forwarding rate of broadcast and multicast packets on each interface. When you configure rate limiting, you are setting the percentage of port bandwidth allowed for a packet type. When the threshold is exceeded, additional packets are discarded.

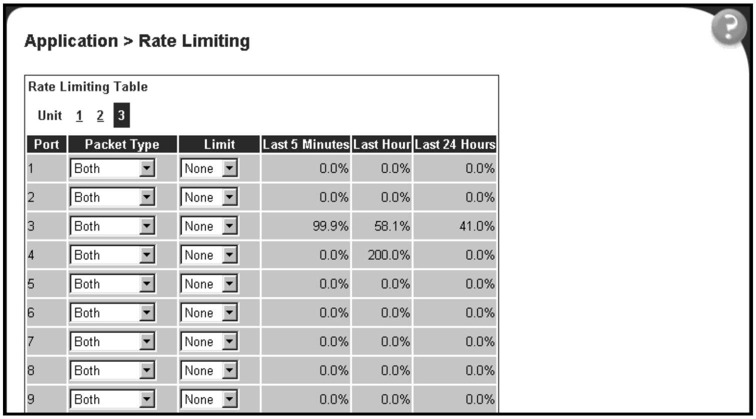
➡ **Note:** If a port is configured for rate limiting, and it is a MultiLink trunk member, all trunk member ports implement rate limiting. If the port becomes disabled, all trunk members become disabled.

To configure rate limiting:

1 From the main menu, choose Application > Rate Limiting.

The Rate Limiting page opens (Figure 71).

Figure 71 Rate Limiting page



Application > Rate Limiting

Rate Limiting Table

Unit 1 2 3

Port	Packet Type	Limit	Last 5 Minutes	Last Hour	Last 24 Hours
1	Both	None	0.0%	0.0%	0.0%
2	Both	None	0.0%	0.0%	0.0%
3	Both	None	99.9%	58.1%	41.0%
4	Both	None	0.0%	200.0%	0.0%
5	Both	None	0.0%	0.0%	0.0%
6	Both	None	0.0%	0.0%	0.0%
7	Both	None	0.0%	0.0%	0.0%
8	Both	None	0.0%	0.0%	0.0%
9	Both	None	0.0%	0.0%	0.0%

Table 57 describes the items on the Rate Limiting page.

Table 57 Rate Limiting page items

Item	Range	Description
Port	1..28	The selected unit's port number. The normal port range is 1 to 28. Note: A standard unit with MDA has a normal range of 25, 26, 28.
Packet Type	(1) Multicast (2) Broadcast (3) Both	Choose the packet type to view on the table. The default setting is Both.
Limit	None, 1-10%	Choose the percentage, if any, of bandwidth allowed for forwarding the packet type specified in the Packet Type field. When the threshold is exceeded, any additional packets are discarded. Note: Rate limiting is disabled if this field is set to none. This allows you to select and view the percentage of specific packet types present in the network, without inadvertently limiting the forwarding rate. The default setting is None.
Last 5 Minutes	0..100%	The percentage of packets received by the port in the last five minutes. This field provides a running average of network activity and is updated every 15 seconds.
Last Hour	0..100%	The percentage of packets received by the port in the last hour. This field provides a running average of network activity and is updated every five minutes.
Last 24 Hours	0..100%	The percentage of packets received by the port in the last 24 hours. This field provides a running average of network activity and is updated every hour.
		Note: The Last 5 Minutes, Last Hour, and Last 24 Hours fields indicate the receiving port's view of network activity regardless of the rate limiting setting.
		Note: When the volume of broadcast and multicast packets is high, placing severe strain on the network (often referred to as a "storm"), you can set the forwarding rate of those packet types to *not exceed* a specified percentage of the total available bandwidth.

2 In the upper-left hand corner, click on the unit number of the device to monitor.

3 Type information in the text boxes, or select from a list.

4 Click Submit.

Note: To avoid broadcast storms (when the volume of a particular packet type is extreme, placing severe strain on the network), set the forwarding rate of the packet type to not exceed a lower percentage of the total available bandwidth.

Configuring IGMP

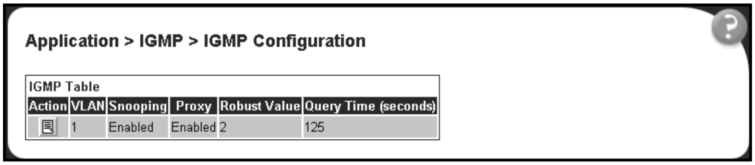
You can configure a VLAN’s switch ports to optimize IP multicast packets in a bridged Ethernet environment, and you can view a table of existing IGMP configurations. For more information about IGMP configuration, see *Using the Business Policy Switch 2000 Software Version 2.0* (208700-C).

To configure IGMP:

1 From the main menu, choose Application > IGMP > IGMP Configuration.

The IGMP Configuration page opens (Figure 72).

Figure 72 IGMP Configuration page



Application > IGMP > IGMP Configuration

IGMP Table

Action	VLAN	Snooping	Proxy	Robust Value	Query Time (seconds)
📝	1	Enabled	Enabled	2	125

Table 58 describes the items on the IGMP Configuration page.

Table 58 IGMP Configuration page items

Item	**Description**
📝	Displays a modification page for the selected VLAN.
VLAN	The number assigned to the VLAN when the VLAN was created. For more information on creating VLANs, see “Creating and managing virtual LANs (VLANs)” on page 171.
Snooping	The operational status for the IGMP snooping feature.
Proxy	If enabled, this feature allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor. Note: This field affects *all* VLANs.

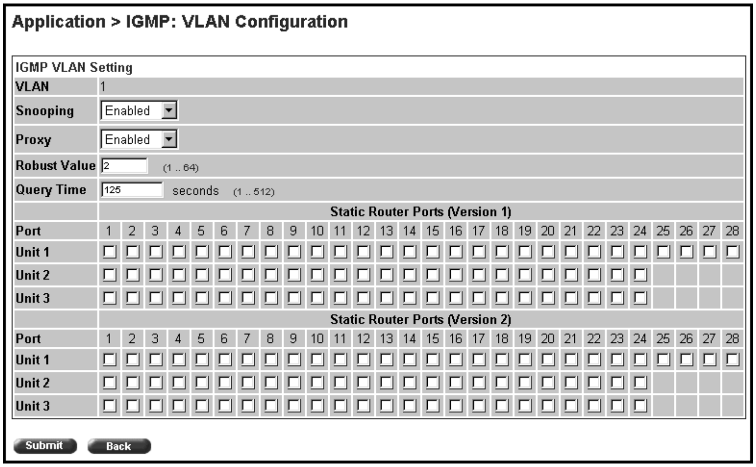
Table 58 IGMP Configuration page items

Item	Description
Robust Value	The predetermined value set by the administrator to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value. Note: This field affects *only* the VLAN specified in the page's VLAN field.
Query Time	The query interval (the interval between general queries sent by the multicast router).

2 In the VLAN row of your choice, click the Modify icon.

The IGMP: VLAN Configuration page opens (Figure 73).

Figure 73 IGMP: VLAN Configuration page



Application > IGMP: VLAN Configuration

IGMP VLAN Setting

VLAN	1
Snooping	Enabled
Proxy	Enabled
Robust Value	2 (1 .. 64)
Query Time	125 seconds (1 .. 512)

Static Router Ports (Version 1)

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				
Unit 3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				

Static Router Ports (Version 2)

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				
Unit 3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐				

Table 59 describes the items on the IGMP: VLAN Configuration page.

Table 59 IGMP: VLAN Configuration page items

Item	Range	Description
VLAN	1..4094	The number assigned to the VLAN when the VLAN was created. For more information on creating VLANs, see "Creating and managing virtual LANs (VLANs)" on page 171.
Snooping	(1) Enabled (2) Disabled	Choose to enable or disable the IGMP snooping feature. Note: This field affects *all* VLANs. The default setting is Enabled.

Table 59 IGMP: VLAN Configuration page items (continued)

Item	**Range**	**Description**
Proxy	(1) Enabled (2) Disabled	Choose to enable or disable the proxy feature. This feature allows the switch to consolidate IGMP Host Membership Reports received on its downstream ports and to generate a consolidated proxy report for forwarding to its upstream neighbor. Note: This field affects *all* VLANs. The default setting is Enabled.
Robust Value	1..64	Type the robust value in the appropriate format. This feature allows you to set the switch to offset expected packet loss on a subnet. If packet losses on a subnet are unacceptably high, the Robust Value field can be increased to a higher value. Note: This field affects *only* the VLAN specified in the page's VLAN field. The default settings is 2.
Query Time	1..512	Type the query time (in seconds) in the appropriate format. This feature allows you to control the number of IGMP messages allowed on the subnet by varying the Query Interval (the interval between general queries sent by the multicast router). Note: This field affects *only* the VLAN specified in the page's VLAN field. The default settings is 125 seconds.
Static Router Ports (Version 1 and Version 2)		Click the check boxes of the router ports to associate with the VLAN (alternatively, click the check box to deselect a selected router port). Note: This field affects *all* VLANs.

3. Type information in the text boxes, or select from a list.
4. In the Static Router Ports section(s), click the check boxes of the router ports to associate with the VLAN.
5. Do one of the following:
    - Click Submit.
    - Click Back to return to the IGMP page without making changes.

    The new configuration is displayed in the IGMP Table (Figure 72).

Viewing Multicast group membership configurations

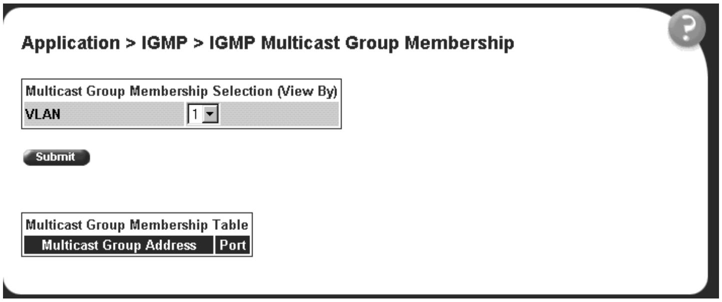
You can view a table configured IP multicast group addresses for a selected VLAN.

To view multicast group membership configurations for a selected VLAN:

1. From the main menu, choose Application > IGMP > IGMP Multicast Group.

   The IGMP Multicast Group Membership page opens (Figure 74).

Figure 74 IGMP Multicast Group Membership page


Application > IGMP > IGMP Multicast Group Membership

Multicast Group Membership Selection (View By)

VLAN 1

Multicast Group Membership Table

Multicast Group Address	Port

Table 60 describes the items on the IGMP Multicast Group Membership page.

Table 60 IGMP Multicast Group Membership page items

Section	Item	Description
Multicast Group Membership Selection (View By)	VLAN	Choose the VLAN on which to view configured IP addresses.
Multicast Group Membership Table	Multicast Group Address	The IP multicast group addresses that are currently active on the associated port.
	Port	The port numbers associated with the IP multicast group addresses displayed in the IP Multicast Group Address field.

2. In the Multicast Group Membership Selection section, choose the number of VLAN on which to view configured IP addresses.
3. Click Submit.

   The results are displayed in the Multicast Group Membership Table (Figure 74).

Creating and managing virtual LANs (VLANs)

A VLAN is a collection of switch ports that make up a single broadcast domain. You can configure a VLAN for a single switch, or for multiple switches. When you create a VLAN, you can control traffic flow and ease the administration of moves, adds, and changes on the network, by eliminating the need to change physical cabling.

Note: For guidelines on configuring VLANs, refer to *Using the Business Policy Switch 2000 Software Version 2.0.*

You can configure three types of VLAN in the Web-based management interface:

- Port-based
- Protocol-based
- MAC SA-based

Beginning with software version 1.2, you can use 256 port-, protocol-, and MAC SA-based VLANs for the stack with a Pure BPS 2000 Stack. (The maximum number of MAC SA-based VLANs available is 48). If you are working with a mixed, or Hybrid, stack, you can use 64 VLANs for the entire stack. When you change from a Pure BPS 2000 Stack mode to a Hybrid Stack mode:

- If you have up to 64 VLANs on the Pure BPS 2000 Stack, they will be retained when you change to a Hybrid Stack.
- If you have more than 64 VLANs on the Pure BPS 2000 Stack, you will lose them all. The Hybrid Stack will return to the default VLAN configuration.

Note: To access 256 VLANs, you must be working in Pure BPS 2000 Stack mode. To view and change the stack operational mode, refer to Chapter 3, “Setting system operational modes.”

Port-based VLANs

A port-based VLAN is a VLAN in which the ports are explicitly configured to be in the VLAN. When you create a port-based VLAN on a switch, you assign a VLAN identification number (VLAN ID) and specify which ports belong to the VLAN. The VLAN ID is used to coordinate VLANs across multiple switches.

With software version 1.1 and higher, the automatic PVID feature automatically sets the PVID when you configure a port-based VLAN. The PVID value will be the same value as VLAN. The user can also manually change the PVID value. The default setting for AutoPVID is Off; you must enable this feature.

Protocol-based VLANs

Beginning with software version 1.2, you can configure as many as 255 protocol-based VLANs, with up to 14 different protocols.

A protocol-based VLAN is a VLAN in which the switch ports are configured as members of a broadcast domain, based on the protocol information within a packet. A protocol-based VLAN can localize broadcast traffic and assure that only the protocol-based VLAN ports are flooded with the specified protocol-type packets.

For protocol-based VLANS, the VLAN classification of the frame is dependent on the protocol of the incoming untagged frame. The frame is forwarded only if that VLAN is registered at the egress port.

MAC SA-based VLANs

A MAC source address (SA)-based VLAN is a VLAN whose frame classification is dependent on the MAC SA of the incoming untagged frame. The frame is forwarded only if that VLAN is registered at the egress port.

Configuring VLANs

You can create VLANs by assigning switch ports, MAC SA, and protocols as VLAN members and you can designate an existing VLAN to act as the management VLAN.

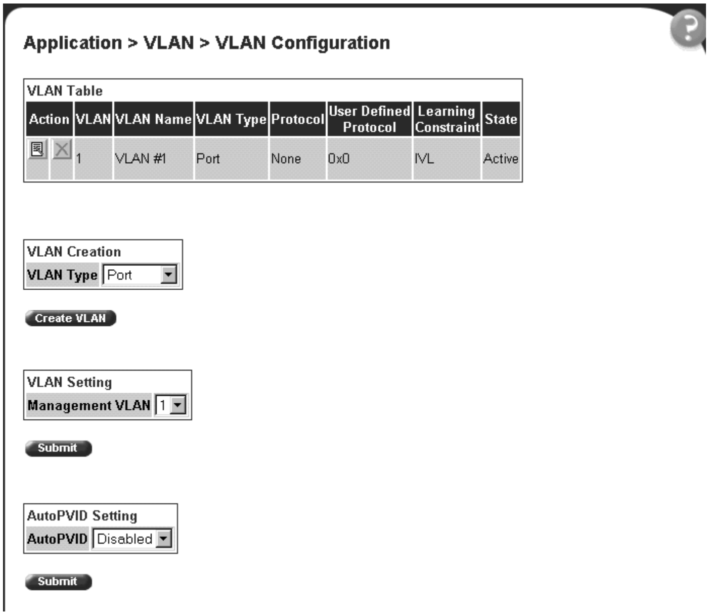
Note: To access the software version 2.0 features in a mixed stack, you must access a BPS 2000 unit. Additionally:
- only 64 VLANS are available in a mixed stack
- multiple STG support is not available in a mixed stack

To open the VLAN Configuration page:

➨ From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 75).

Figure 75 VLAN Configuration page



Application > VLAN > VLAN Configuration

VLAN Table

Action	VLAN	VLAN Name	VLAN Type	Protocol	User Defined Protocol	Learning Constraint	State
🖹 ☒	1	VLAN #1	Port	None	0x0	IVL	Active

VLAN Creation

VLAN Type Port

VLAN Setting

Management VLAN 1

AutoPVID Setting

AutoPVID Disabled

Table 61 describes the items on the VLAN Configuration page.

Table 61 VLAN Configuration page items

Section	**Item**	**Description**
VLAN Table	📝	Displays a modification page.
	✖	Deletes the row.
	VLAN	The number assigned to the VLAN when the VLAN was created.
	VLAN Name	The name assigned to the VLAN when the VLAN was created.
	VLAN Type	The base-type assigned when the VLAN was created. The base types are: Port-based, IP Subnet-based, Protocol-based, and MAC SA-based.
	Protocol	The protocol assigned when the VLAN was created. The protocol types are: IP, IPX 802.2, 1PX 802.3, IPX Snap, IPX Ethernet II, Apple Talk, DEC Lat, SNA 802.2, SNA Ethernet II, Net Bios, XNS, Vines, Ipv6, User Defined, and RARP. For more information, see Table 65 on page 180.
	User Defined Protocol	The user-defined protocol assigned when the VLAN was created.
	Learning Constraint	The type of learning constraint selected when the VLAN was created. The choices are IVL and SVL. Note: If you select IVL, the VLAN uses an independent filtering database from all other VLANs. If you select SVL, the VLAN shares the same filtering database as all other VLANs with SVL. Note: When the stack mode is set to “Pure BPS 2000,” the default setting is IVL; IVL is available *only* with a Pure BPS 2000 stack mode. When the stack mode is set to “Hybrid,” the default setting is SVL.
	State	The current operational state of the VLAN.
VLAN Creation	VLAN Type	Choose the type of VLAN to create and click Create VLAN. Your options are: port-based (page 175), protocol-based (page 178), and MAC SA-based (page 183).
VLAN Setting	Management VLAN	Choose the VLAN to designate as the management VLAN.
AutoPVID Setting	AutoPVID	Choose Enabled to activate the Automatic PVID feature and click Submit. Note: Use this *only* with port-based VLANs.

Creating a port-based VLAN

To create a port-based VLAN:

1 From the main menu choose Application > VLAN > VLAN Configuration.

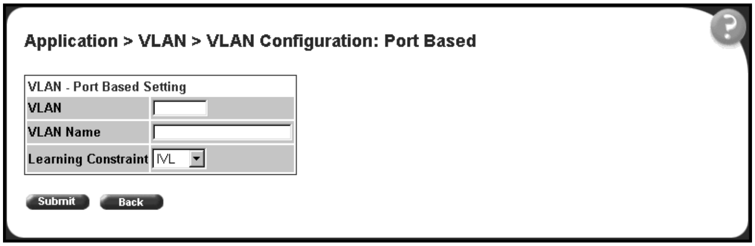
The VLAN Configuration page opens (Figure 75).

2 In the VLAN Creation section, choose Port.

3 Click Create VLAN.

The VLAN Configuration: Port Based setting page opens (Figure 76).

Figure 76 VLAN Configuration: Port Based setting page



Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting	
VLAN	
VLAN Name	
Learning Constraint	IVL

Table 62 describes the items on the VLAN Configuration: Port Based setting page.

Table 62 VLAN Configuration: Port Based setting page items

Item	Range	Description
VLAN	1..4094	The number assigned to the VLAN when the VLAN was created.
VLAN Name	1..16	Type a character string to create a unique name to identify the VLAN, for example, VLAN1.
Learning Constraint	(1) IVL (2) SVL	Choose your learning constraint type. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL. Note: If the stack is set to a “pure” operational mode, the default setting is IVL; IVL is available *only* with Pure BPS 2000 stack operational mode. If the stack is set to a “hybrid” operational mode, the default setting is SVL. For more information on setting your stack operational mode, see “Setting system operational modes” on page 128.

4 Type information in the text boxes, or select from a list.

5 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The new port-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page (Figure 75).

Modifying a port-based VLAN

To modify an existing port-based VLAN:

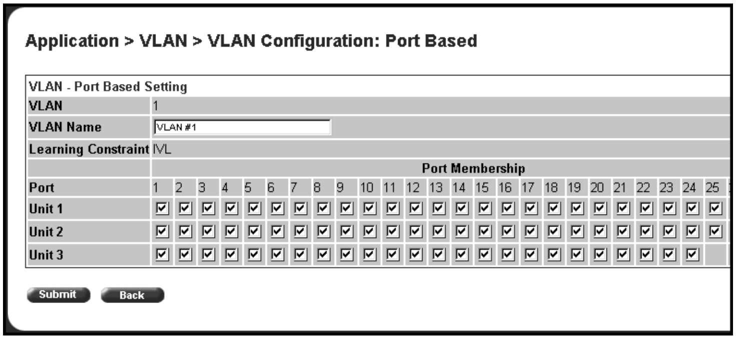
1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 75).

2 In the VLAN Table section, in the port-based VLAN row of your choice, click the Modify icon.

The VLAN Configuration: Port Based modification page opens (Figure 77).

Figure 77 VLAN Configuration: Port Based modification page



Application > VLAN > VLAN Configuration: Port Based

VLAN - Port Based Setting

VLAN	1
VLAN Name	VLAN #1
Learning Constraint	IVL

Port Membership

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Unit 1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Unit 2	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Unit 3	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	

Table 63 describes the items on the VLAN Configuration: Port Based modification page.

Table 63 VLAN Configuration: Port Based modification page items

Item	**Description**
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
Learning Constraint	The type of learning constraint selected when the VLAN was created. The learning constraint choices are IVL and SVL. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. IVL is available *only* in the Pure BPS 2000 stack operational mode. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL.
Port/Port Membership	Click the check boxes of *standalone or stacked unit* ports to associate it with the VLAN or, if the port is already a member, click the check box to deselect the it as a member of the VLAN. A port can be configured in one or more VLANs. This field is dependent on the Tagging field value in the VLAN Port Configuration screen. For example: • When the Tagging field is set to *Untagged Access*, you can set the Port Membership field as an untagged port member or as a non-VLAN port member. • When the Tagging field is set to *Tagged Trunk*, you can set the Port Membership field as a tagged port member or as a non-VLAN port member.

3 Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.

4 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table (Figure 75).

Creating a protocol-based VLAN

To create a protocol-based VLAN:

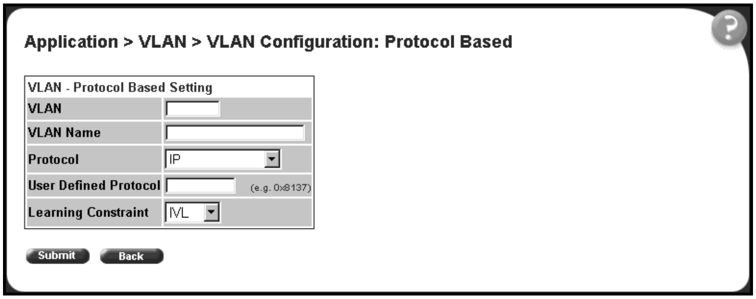
1. From the main menu, choose Application > VLAN > VLAN Configuration.

   The VLAN Configuration page opens (Figure 75).

2. In the VLAN Creation section, choose Protocol.
3. Click Create VLAN.

   The VLAN Configuration: Protocol Based setting page opens (Figure 78).

Figure 78 VLAN Configuration: Protocol Based setting page



Application > VLAN > VLAN Configuration: Protocol Based

VLAN - Protocol Based Setting	
VLAN	
VLAN Name	
Protocol	IP
User Defined Protocol	(e.g. 0x8137)
Learning Constraint	IVL

Table 64 describes the items on the VLAN Configuration: Protocol Based setting page.

Note: Beginning with software version 1.2, there are 14 available protocols.

Table 64 VLAN Configuration: Protocol Based setting page items

Item	Range	Description
VLAN	1..4094	Type a unique number to identify the VLAN.
VLAN Name	1..16	Type a unique name to identify the VLAN.
Protocol	IP, IPX 802.2, 1PX 802.3, IPX Snap, IPX Ethernet II, Apple Talk, DEC Lat, SNA 802.2, SNA Ethernet II, Net Bios, XNS, Vines, Ipv6, User Defined, and RARP.	Choose the supported protocol for the VLAN. For more information, see Table 65 on page 180.
User Defined Protocol		If you selected “User Defined” from the Protocol pulldown list, specify the protocol identifier for the VLAN. Note: Any frames that match the specified PID, in any of the following ways are assigned to that user defined VLAN: • The ethertype for Ethernet type 2 frames • The PID in Ethernet SNAP frames • The DSAP or SSAP value in Ethernet 802.2 frames. For a list of rereserved PIDs that are unavailable for user-defined PIDs, see Table 66 on page 181.
Learning Constraint	(1) IVL (2) SVL	Choose your learning constraint type. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL. Note: If the stack is set to a “pure” operational mode, the default setting is IVL; IVL is available *only* in Pure BPS 2000 stack operational mode. If the stack is set to a “hybrid” operational mode, the default setting is SVL. For more information on setting your stack operational mode, see “Setting system operational modes” on page 128.

4 Type information in the text boxes, or select from a list.

5 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The new protocol-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page (Figure 75).

Caution: BayStack 450-!GBIC, 450-1SR, 450-1SX, 450-1LR, 450-LX MDA ports and BayStack 410 ports do not have the ability to assign incoming untagged frames to a protocol-based VLAN. To allow gigabit ports and BayStack 410 ports to participate in protocol-based VLANs, set the tagging field value to "Tagged Trunk" (see "Configuring broadcast domains" on page 188).

Table 65 defines the standard protocol-based VLANs and PID types that are supported by the Business Policy Switch and BayStack 450 and 410 switches. See Table 66 for a list of rereserved PIDS that are not available for user-defined PIDs.

Table 65 Standard protocol-based VLANs and PID types

PID Name	**Encapsulation**	**PID Value (hex)**	**VLAN Type**
IP Ether2	Ethernet type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
Ipx 802.3	Ethernet 802.2	FF FF	Novell IPX on Ethernet 802.3 frames
Ipx 802.2	Ethernet 802.0	E0 E0	Novell IPX on Ethernet 802.2 frames
Ipx Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames
Ipx Ethernet II	Ethernet type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
Apple Talk	Ethernet type 2 or Ethernet Snap	809B, 80F3	AppleTalk on Ethernet Type 2 and Ethernet Snap frames
DEC Lat	Ethernet type 2	6004	DEC LAT protocol
DEC Other	Ethernet type 2	6000 - 6003, 6005 - 6009, 8038	Other DEC protocols
Sna 802.2	Ethernet 802.2	04**, **04	IBM SNA on IEEE 802.2 frames
Sna Ethernet II	Ethernet type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios	Ethernet type 2	F0**, **F0	NetBIOS protocol
XNS	Ethernet type 2	0600, 0807	Xerox XNS
Vines	Ethernet type 2	0BAD	Banyan VINES
IPv6	Ethernet type 2	86DD	IP version 6

Table 65 Standard protocol-based VLANs and PID types (continued)

PID Name	Encapsulation	PID Value (hex)	VLAN Type
RARP	Ethernet type 2	8035	Reverse Address Resolution Protocol (RARP): RARP is a protocol used by some old diskless devices to obtain IP addresses by providing the MAC layer address. When you create a VLAN based on RARP, you can limit the RARP broadcasts to the ports that lead to the RARP server.
User-Defined	Ethernet type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16 bit value	If you select “User Defined” from the Protocol pulldown list, specify the protocol identifier for the VLAN. Note: Any frames that match the specified PID, in any of the following ways are assigned to that user defined VLAN: The ethertype for Ethernet type 2 frames The PID in Ethernet SNAP frames The DSAP or SSAP value in Ethernet 802.2 frames. For a list of rereserved PIDs that are unavailable for user-defined PIDs, see Table 65 on page 180

Table 66, describes the PIDS that are reserved and not available for user-defined PIDs.

Table 66 Predefined Protocol Identifier (PID)

PID Name	Encapsulation	PID Value (hex)	VLAN Type
IP Ether2	Ethernet type 2	0800, 0806	Standard IP on Ethernet Type 2 frames
Ipx 802.3	Ethernet 802.2	FF FF	Novell IPX on Ethernet 802.3 frames
Ipx 802.2	Ethernet 802.0	E0 E0	Novell IPX on Ethernet 802.2 frames
Ipx Snap	Ethernet Snap	8137, 8138	Novell IPX on Ethernet SNAP frames
Ipx Snap2	Ethernet type 2	8137, 8138	Novell IPX on Ethernet Type 2 frames
AplTk Ether2 Snap	Ethernet type 2 or Ethernet Snap	809B, 80F3	AppleTalk on Ethernet Type 2 and Ethernet Snap frames
Declat Ether2	Ethernet type 2	6004	DEC LAT protocol
DecOther Ether2	Ethernet type 2	6000 - 6003, 6005 - 6009, 8038	Other DEC protocols
Sna 802.2	Ethernet 802.2	04**, **04	IBM SNA on IEEE 802.2 frames
Sna Ether2	Ethernet type 2	80D5	IBM SNA on Ethernet Type 2 frames
NetBios 802.2	Ethernet type 2	F0**, **F0	NetBIOS protocol
Xns Ether2	Ethernet type 2	0600, 0807	Xerox XNS

Table 66 Predefined Protocol Identifier (PID) (continued)

Vines Ether2	Ethernet type 2	0BAD	Banyan VINES
Ipv6 Ether2	Ethernet type 2	86DD	IP version 6
User-Defined	Ethernet type 2, Ethernet 802.2, or Ethernet Snap	User-defined 16 bit value	User-defined protocol-based VLAN. For a list of rereserved PIDs that are unavailable for user-defined PIDs, see Table 66 on page 181.

Modifying a protocol-based VLAN

To modify an existing protocol-based VLAN:

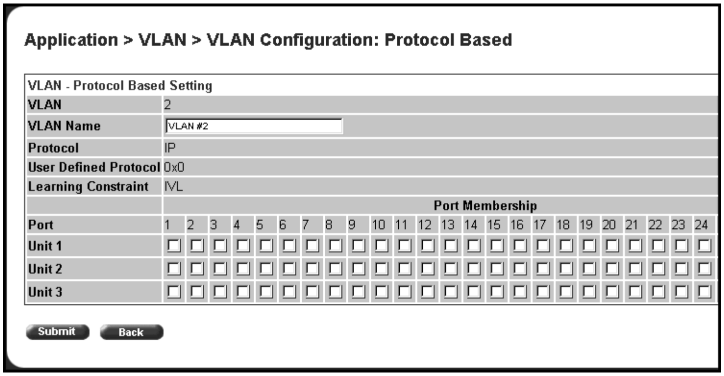
1. From the main menu, choose Application > VLAN > VLAN Configuration.

   The VLAN Configuration page opens (Figure 75).

2. In the VLAN Table section, in the protocol-based VLAN row of your choice, click the Modify icon.

   The VLAN Configuration: Protocol Based modification page opens (Figure 79).

Figure 79 VLAN Configuration: Protocol Based modification page



Application > VLAN > VLAN Configuration: Protocol Based

VLAN - Protocol Based Setting

VLAN	2
VLAN Name	VLAN #2
Protocol	IP
User Defined Protocol	0x0
Learning Constraint	IVL

	Port Membership																							
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Table 67 describes the items on the VLAN Configuration: Protocol Based modification page.

Table 67 VLAN Configuration: Protocol Based modification page items

Item	Description
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
Learning Constraint	The type of learning constraint selected when the VLAN was created. The learning constraint choices are IVL and SVL. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. IVL is available *only* in Pure BPS 2000 stack operational mode.If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL.
Port/Port Membership	Click the check boxes beneath a port to associate the port with the VLAN or, if the port is already selected click the check box to deselect the port as a member of the VLAN.

3. Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.
4. Do one of the following:
    - Click Submit.
    - Click Back to return to the VLAN Configuration page without making changes.

   The modified VLAN configuration is displayed in the VLAN Table (Figure 75).

Creating a MAC SA-based VLAN

To create a MAC SA-based VLAN:

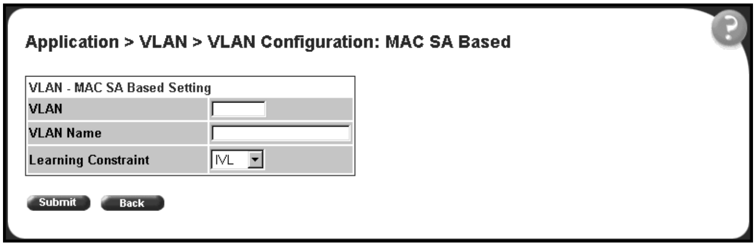
1. From the main menu, choose Application > VLAN > VLAN Configuration.

   The VLAN Configuration page opens (Figure 75).

2. In the VLAN Creation section, choose MAC SA.
3. Click Create VLAN.

   The VLAN Configuration: MAC SA Based setting page opens (Figure 80).

Figure 80 VLAN Configuration: MAC SA Based setting page



Application > VLAN > VLAN Configuration: MAC SA Based

VLAN - MAC SA Based Setting	
VLAN	
VLAN Name	
Learning Constraint	IVL

Table 68 describes the items on the VLAN Configuration: MAC SA Based setting page.

Table 68 VLAN Configuration: MAC SA Based setting page items

Item	**Range**	**Description**
VLAN	1..4094	Type a unique number to identify the VLAN.
VLAN Name	1..16	Type a unique name to identify the VLAN, for example *.
Learning Constraint	(1) IVL (2) SVL (default)	Choose your learning constraint type. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL. Note: If the stack is set to a “pure” operational mode, the default setting is IVL; IVL is available *only* in Pure BPS 2000 mode. If the stack is set to a “hybrid” operational mode, the default setting is SVL. For more information on setting your stack operational mode, see “Setting system operational modes” on page 128.

4 Type information in the text boxes, or select from a list.

5 Do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The new MAC SA-based VLAN configuration appears in the VLAN Table on the VLAN Configuration page (Figure 75).

Modifying a MAC SA-based VLAN

To modify an existing MAC SA-based VLAN:

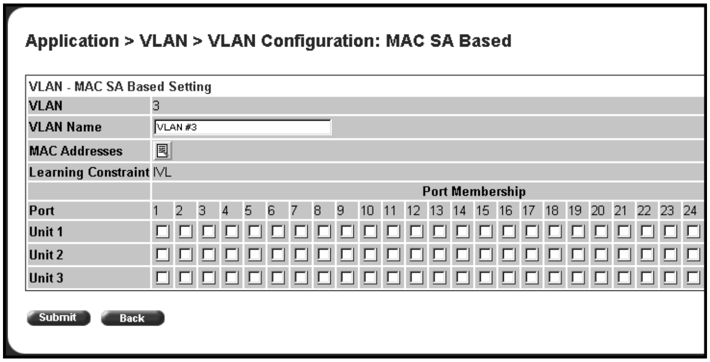
1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 75).

2 In the VLAN Table section, in the MAC SA-based VLAN row of your choice, click the Modify icon.

The VLAN Configuration: MAC SA Based modification page opens (Figure 81).

Figure 81 VLAN Configuration: MAC SA Based modification page



Application > VLAN > VLAN Configuration: MAC SA Based

VLAN - MAC SA Based Setting	
VLAN	3
VLAN Name	VLAN #3
MAC Addresses	🗎
Learning Constraint	IVL

	Port Membership																							
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 2	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Unit 3	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐

Table 69 describes the items on the VLAN Configuration: MAC SA Based modification page.

Table 69 VLAN Configuration: MAC SA Based modification page items

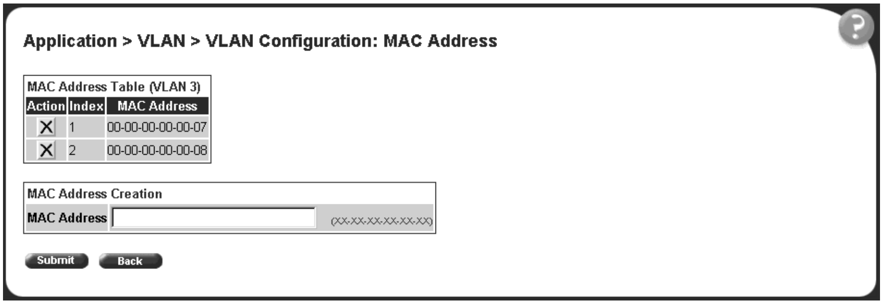
Item	Description
VLAN	The number assigned to the VLAN when the VLAN was created.
VLAN Name	(Re)name the VLAN.
📝	Opens the VLAN Configuration: MAC Address page (Figure 82).
Learning Constraint	The type of learning constraint selected when the VLAN was created. The learning constraint choices are IVL and SVL. Note: If IVL is selected, the VLAN uses an independent filtering database from all other VLANs. IVL is available *only* in the Pure BPS 2000 stack operational mode. If SVL is selected, the VLAN shares the same filtering database as all other VLANs with SVL.

3 Type information in the text boxes, or click the check box of a port to associate it with the VLAN or, if the port is already a member, click the check box to deselect it as a member of the VLAN.

4 To create MAC address associations, click the modify icon.

The VLAN Configuration: MAC Address page opens (Figure 82).

Figure 82 VLAN Configuration: MAC Address page



Application > VLAN > VLAN Configuration: MAC Address

MAC Address Table (VLAN 3)

Action	Index	MAC Address
☒	1	00-00-00-00-00-07
☒	2	00-00-00-00-00-08

MAC Address Creation

MAC Address (XX-XX-XX-XX-XX-XX)

5 In the MAC Address Creation section, type the MAC address to associate with the VLAN.

The MAC address appears in the MAC Address Table (Figure 82).

Note: You can delete an existing MAC address by clicking the delete icon in the row of the MAC address you want to delete.

---

6 Do one of the following:

- Click Submit to save your changes and return to the VLAN Configuration: MAC SA Based setting page.
- Click Back to return to the VLAN Configuration: MAC SA Based setting page without making changes.

7 On the VLAN Configuration: MAC SA Based setting page, do one of the following:

- Click Submit.
- Click Back to return to the VLAN Configuration page without making changes.

The modified VLAN configuration is displayed in the VLAN Table (Figure 75).

Selecting a management VLAN

You can select any VLAN to perform as the management VLAN. VLAN 1 is the default management VLAN for the switch. To set this field, the VLAN State field value must be active.

To select a VLAN as the management VLAN:

1 From the main menu, choose Application > VLAN > VLAN Configuration.

The VLAN Configuration page opens (Figure 75).

2 In the VLAN Setting section, choose the VLAN to assign as your management VLAN.

3 Click Submit.

Deleting a VLAN configuration

To delete a VLAN configuration:

1. From the main menu, choose Application > VLAN > VLAN Configuration.

   The VLAN Configuration page opens (Figure 75).

2. In the VLAN Table, click the Delete icon for the entry you want to delete.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the VLAN configuration.
   - Click Cancel to return to the VLAN Configuration page without making changes.

Note: You cannot delete VLAN 1.

Configuring broadcast domains

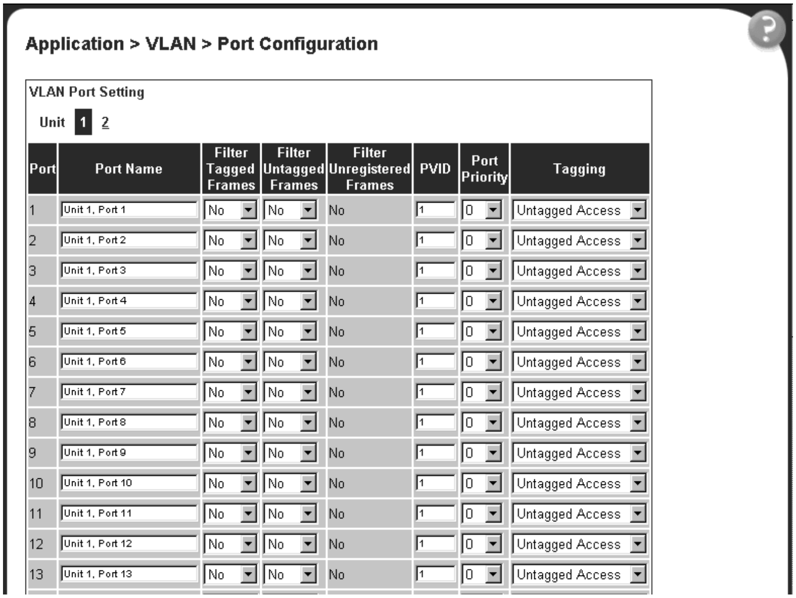
You can configure specified VLAN switch ports with the appropriate PVID/VLAN association that enables the creation of broadcast domains. If you have enabled automatic PVID, you can change the PVID number on this screen. You can configure specified switch ports to filter (discard) all received tagged frames, untagged frames, or unregistered frames. You can also prioritize the order in which the switch forwards untagged packets, on a per-port basis.

To configure broadcast domains:

1. From the main menu, choose Application > VLAN > Port Configuration.

   The Port Configuration page opens (Figure 83).

Figure 83 Port Configuration page



Application > VLAN > Port Configuration

VLAN Port Setting

Unit **1** 2

Port	Port Name	Filter Tagged Frames	Filter Untagged Frames	Filter Unregistered Frames	PVID	Port Priority	Tagging
1	Unit 1, Port 1	No	No	No	1	0	Untagged Access
2	Unit 1, Port 2	No	No	No	1	0	Untagged Access
3	Unit 1, Port 3	No	No	No	1	0	Untagged Access
4	Unit 1, Port 4	No	No	No	1	0	Untagged Access
5	Unit 1, Port 5	No	No	No	1	0	Untagged Access
6	Unit 1, Port 6	No	No	No	1	0	Untagged Access
7	Unit 1, Port 7	No	No	No	1	0	Untagged Access
8	Unit 1, Port 8	No	No	No	1	0	Untagged Access
9	Unit 1, Port 9	No	No	No	1	0	Untagged Access
10	Unit 1, Port 10	No	No	No	1	0	Untagged Access
11	Unit 1, Port 11	No	No	No	1	0	Untagged Access
12	Unit 1, Port 12	No	No	No	1	0	Untagged Access
13	Unit 1, Port 13	No	No	No	1	0	Untagged Access

Table 70 describes the items on the Port Configuration page.

Table 70 Port Configuration page items

Item	Range	Description
Port	1..28	The port number.
Port Name	1..16	Type character string to create a unique port name, for example, Unit 1, Port 1.
Filter Tagged Frames	(1) Yes (2) No	Choose how to process filter tagged frames. When a flag is set (Yes), the frames are discarded by the forwarding process. When the flag is reset, the frames are processed normally. The default setting is No (frames are not discarded).
Filter Untagged Frames	(1) Yes (2) No	Choose how to process filter untagged frames. When a flag is set, the frames are discarded by the forwarding process. The default setting is No (no frames discarded).
Filter Unregistered Frames	(1) Yes (2) No	Displays yes/no if a flag is set. If yes, unregistered frames are discarded by the forwarding process. When the flag is reset, unregistered frames are processed normally. The default settings is No.

Table 70 Port Configuration page items (continued)

Item	Range	Description
PVID	1..4094	Type the number of the VLAN ID to assign to untagged frames received on this trunk port. For example, a port with a PVID of 3 assigns all untagged frames received on this port to VLAN 3. The default setting is 1. Note: If AutoPVID is enabled and you want another PVID, enter the desired PVID here.
Port Priority	0-7	Choose the level of priority for each port.
Tagging	(1) Untagged Access (2) Tagged Trunk	Choose the tagging for each port.

2. In the upper-left hand corner, click on the unit number of the switch to monitor.
3. Type information in the text boxes, or select from a list.
4. Click Submit.

Viewing VLAN port information

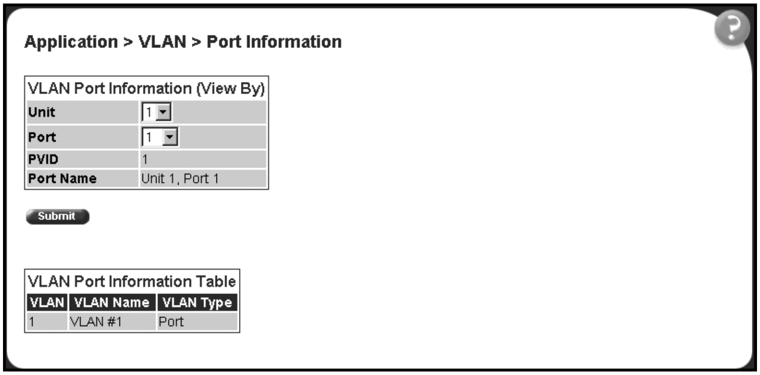
You can view VLAN information about a selected switch port.

To view VLAN port information:

1. From the main menu, choose Application > VLAN > Port Information.

   The Port Information page opens (Figure 84).

Figure 84 Port Information page



Application > VLAN > Port Information

VLAN Port Information (View By)	
Unit	1
Port	1
PVID	1
Port Name	Unit 1, Port 1

VLAN Port Information Table

VLAN	VLAN Name	VLAN Type
1	VLAN #1	Port

Table 71 describes the items on the Port Information page.

Table 71 Port Information page items

Section	Item	Range	Description
VLAN Port Information (View By)	Unit	1..8	Choose the number of the switch to view.
	Port	1..28	Choose the number of the switch's port to view.
	PVID		The PVID assigned when the VLAN port was created.
	Port Name		The port name assigned when the VLAN port was created.
VLAN Port Information Table	VLAN		The number assigned to the VLAN when it was created.
	VLAN Name		The name assigned to the VLAN when it was created.
	VLAN Type		The VLAN type assigned to the VLAN when it was created.

2 In the VLAN Port Information (View By) section, enter the unit and port number of the VLAN you want to view.

3 Click Submit.

The results of your request are displayed in the VLAN Port Information Table (Figure 84).

Managing spanning tree groups

You can configure system parameters for Spanning Tree Protocol, the industry standard for avoiding loops in switched networks. You can configure individual switch ports or all switch ports for participation in the spanning tree algorithm (STA).

Note: STP resolves duplicate paths in networks and is not necessary for ports that have workstations directly attached to the switch. When STP is enabled on these ports (the default), workstations are unable to attach to servers for a few seconds while STP stabilizes.

With software version 1.2 and higher, the BPS 2000 supports multiple instances (8) of spanning tree groups (STGs) running simultaneously, either all in one standalone switch or across a Pure BPS 2000 Stack. Each STG sends its own Bridge Protocol Data Units (BPDUs), and each STG must be independently configured.

With software version 2.0, you can choose which VLAN in the STG will send the tagged BPDU.

Note: You must be in Pure BPS 2000 Stack mode in the Stack Operational Mode screen to enable more than 1 STG. If you change to Hybrid mode, you lose all but the default STG.

In the default configuration of the BPS 2000, a single STG with the ID of 1 includes all ports on the switch. It is called the Default STG and sends only untagged BPDUs in order to operate with all devices that support only one instance of STP. Although ports can be added to or deleted from the Default STG, the Default STG itself **cannot** be deleted from the system. All other STGs, except the Default STG, must be created by the user.

Note: To become active, each STG must be enabled by the user after creation. For guidelines on configuring, refer to *Using the Business Policy Switch 2000 Software Version 2.0.*

Beginning with software version 2.0, you can set the spanning tree priority and path cost for each individual port.

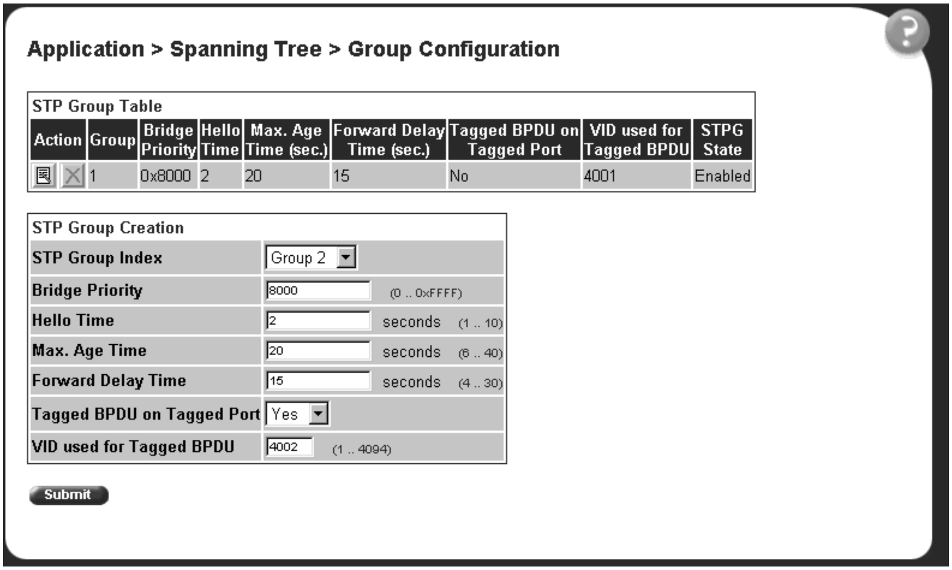
Creating spanning tree groups

To configure spanning tree groups:

1 From the main menu, choose Application > Spanning Tree > Group Configuration.

The Group Configuration page opens (Figure 85).

Figure 85 Spanning Tree Group Configuration page



Application > Spanning Tree > Group Configuration

STP Group Table

Action	Group	Bridge Priority	Hello Time	Max. Age Time (sec.)	Forward Delay Time (sec.)	Tagged BPDU on Tagged Port	VID used for Tagged BPDU	STPG State
✎ ☒	1	0x8000	2	20	15	No	4001	Enabled

STP Group Creation

STP Group Index	Group 2 ▾	
Bridge Priority	8000	(0 .. 0xFFFF)
Hello Time	2	seconds (1 .. 10)
Max. Age Time	20	seconds (6 .. 40)
Forward Delay Time	15	seconds (4 .. 30)
Tagged BPDU on Tagged Port	Yes ▾	
VID used for Tagged BPDU	4002	(1 .. 4094)

Table 72 describes the items on the Spanning Tree Group Configuration page.

Table 72 Spanning Tree Group Configuration page items

Section	Item	Description
STP Group Table	☒	Deletes the group.
	Group	The number assigned to the spanning tree group when the group was created.

Table 72 Spanning Tree Group Configuration page items

Section	**Item**	**Description**
	Bridge Priority	For the STP Group, indicates the management-assigned priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The spanning tree algorithm uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values.
	Hello Time	For the STP Group, indicates the Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note that, although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network.
	Max. Age time (sec.)	For the STP Group, specifies the maximum age (in seconds) that a Hello message can attain before it is discarded. This parameter, specified by management for this bridge, takes effect only when the bridge becomes the root bridge. Note that, if this bridge becomes the root bridge, its Maximum Age Time parameter value becomes the Actual Maximum Age Time parameter value for all bridges participating in the spanning tree network.
	Forward Delay Time (sec.)	For the STP Group indicates the Forward Delay parameter value specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. The Forward Delay parameter value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note that all bridges participating in the spanning tree network use the root bridge's Forward Delay parameter value.
	Tagged BPDU on Tagged Port	Displays whether you are sendin]g either tagged or untagged BPDUs from a tagged port.
	VID used for Tagged BPDU	Displays the VLAN ID you are sending the tagged BPDUs for the specified STG to.
	STPG State	The current operational state of the spanning tree group: Enabled or Disabled.
STP Group Creation	STP Group Index	Choose the group number you want to create.
	Bridge Priority	Enter the priority you want.
	Hello Time	Enter the hello time you want for this STG in seconds; range is 1 to 10.
	Max. Age time (sec.)l	Enter the maximum age time you want for this STG in seconds; range is 6 to 40.
	Forward Delay Time (sec.)	Enter the forward delay time you want for this STG in seconds; range is 4 to 30.
	Tagged BPDU on Tagged Port	Set the frames as tagged (Yes) or untagged (No) on tagged ports.
	VID used for Tagged BPDU	Enter the VLAN ID you want to send the tagged BPDUs for the specified STG. Note: The default VIDs are 4001 through 4008 for STG 1 through 8, respectively.

2 Complete the fields as shown.

3 Click Submit.

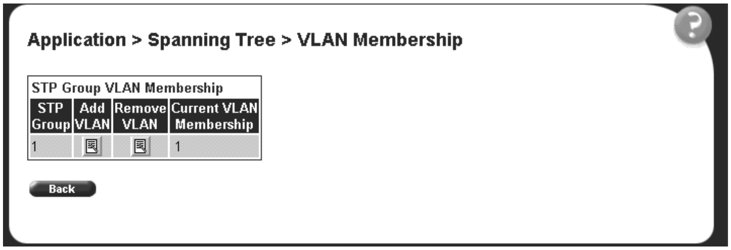
Associating STG with VLAN membership

To add a VLAN to an STG:

1 From the main menu, choose, Application > Spanning Tree > VLAN Membership.

The Spanning Tree VLAN Membership page opens (Figure 86).

Figure 86 Spanning Tree VLAN Membership page



Application > Spanning Tree > VLAN Membership

STP Group VLAN Membership

STP Group	Add VLAN	Remove VLAN	Current VLAN Membership
1	▤	▤	1

The table displays the spanning tree group and the current VLAN membership.

You can add or remove one or more VLANs to an STG.

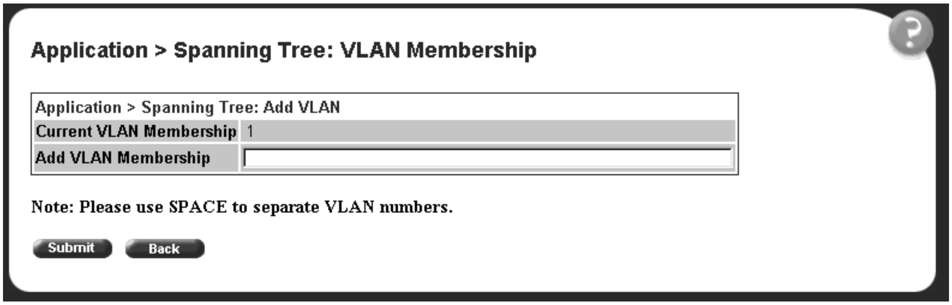
Note: Beginning with software version 2.0, you can move a VLAN from one STG to another by simply adding the VLAN to the specified STG. You no longer must remove the VLAN from the previous STG first.

2 To add a VLAN:

a Click the modification icon in the Add VLAN column.

The Spanning Tree VLAN Membership Add VLAN page opens (Figure 87).

Figure 87 Spanning Tree Add VLAN page



Application > Spanning Tree: VLAN Membership

Application > Spanning Tree: Add VLAN	
Current VLAN Membership	1
Add VLAN Membership	

Note: Please use SPACE to separate VLAN numbers.

b Enter the number of the VLAN(s) you want to add to the STG.

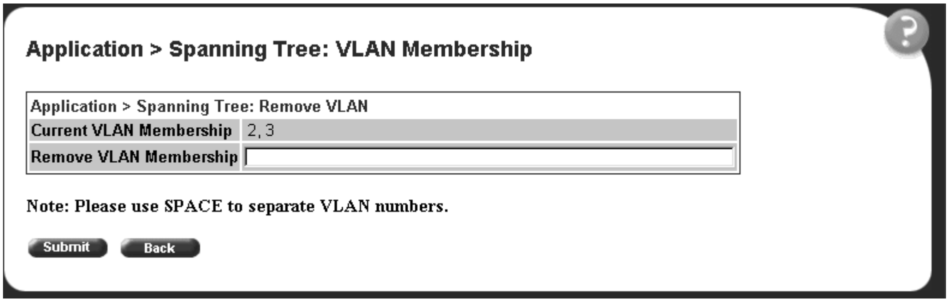
c Click Submit.

3 To remove a VLAN:

a Click the modification icon in the Remove VLAN column.

The Spanning Tree VLAN Membership Remove VLAN page opens (Figure 88).

Figure 88 Spanning Tree Remove VLAN page



Application > Spanning Tree: VLAN Membership

Application > Spanning Tree: Remove VLAN	
Current VLAN Membership	2, 3
Remove VLAN Membership	

Note: Please use SPACE to separate VLAN numbers.

b Enter the number of the VLAN(s) you want to remove to the STG.

c Click Submit.

Note: You cannot delete VLAN 1 from STG 1.

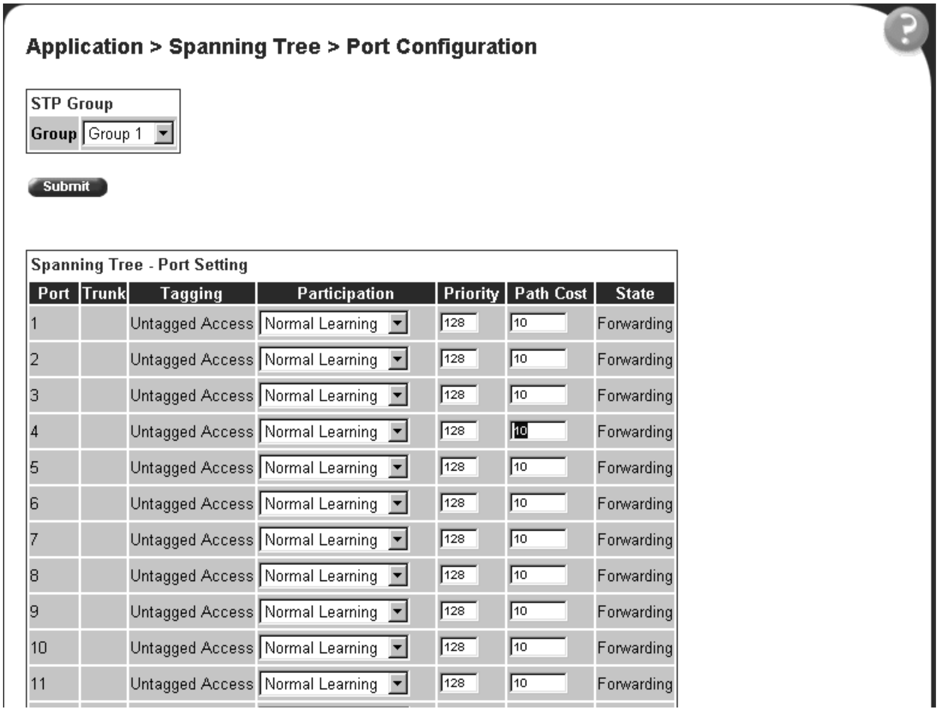
Configuring ports for spanning tree

To configure switch ports for Spanning Tree participation:

1 From the main menu, choose Application > Spanning Tree > Port Configuration.

The Spanning Tree Port Configuration page opens (Figure 89).

Figure 89 Spanning Tree Port Configuration page



Application > Spanning Tree > Port Configuration

STP Group

Group: Group 1

Spanning Tree - Port Setting

Port	Trunk	Tagging	Participation	Priority	Path Cost	State
1		Untagged Access	Normal Learning	128	10	Forwarding
2		Untagged Access	Normal Learning	128	10	Forwarding
3		Untagged Access	Normal Learning	128	10	Forwarding
4		Untagged Access	Normal Learning	128	10	Forwarding
5		Untagged Access	Normal Learning	128	10	Forwarding
6		Untagged Access	Normal Learning	128	10	Forwarding
7		Untagged Access	Normal Learning	128	10	Forwarding
8		Untagged Access	Normal Learning	128	10	Forwarding
9		Untagged Access	Normal Learning	128	10	Forwarding
10		Untagged Access	Normal Learning	128	10	Forwarding
11		Untagged Access	Normal Learning	128	10	Forwarding

Table 73 describes the items on the Spanning Tree Port Configuration page.

Table 73 Spanning Tree Port Configuration page items

Section	Item	Description
STP Group	Group	Choose the STG Group you want to view.
Spanning Tree - Port Setting	Port	The port number of the currently displayed unit.
	Trunk	The trunk that corresponds to the switch ports specified as MLT members.
	Tagging	Displays whether the port is a tagged or an untagged port.
	Participation	Choose any (or all) of the switch ports for Spanning Tree participation.Your options are: (1) Normal Learning (2) Fast Learning (3) Disabled Note: When an individual port is a trunk member, changing this setting for one of the trunk members changes the setting for all members of that trunk. Consider the effect changing this value has in your network topology before making changes. The default settings is Normal Learning.
	Priority	The bridge spanning tree parameter that prioritizes the port's lowest path cost to the root. When one or more ports have the same path cost, the STA selects the path with the highest priority (lowest numerical value).
	Path Cost	The bridge spanning tree parameter that determines the lowest path cost to the root.
	State	The current state of the port as defined by application of the Spanning Tree Protocol. This state controls what action a port takes on reception of a frame. Note: If the bridge has detected a port that is malfunctioning, it will place that port into the broken (6) state. For ports which are disabled, this object will have a value of disabled (1).

2 Using the Spanning Tree - Port Settings fields, in the port row(s) of your choice, choose to enable STP (normal learning or fast learning) or disable STP.

3 Enter the spanning tree priority value for the specified port.

You do not have to enter a value if you want to use the default priority of 128.

4 Enter the spanning tree path cost value for the specified port.

You do not have to enter a value if you want to use the default path cost of 10.

5 Click Submit.

Changing spanning tree bridge switch settings

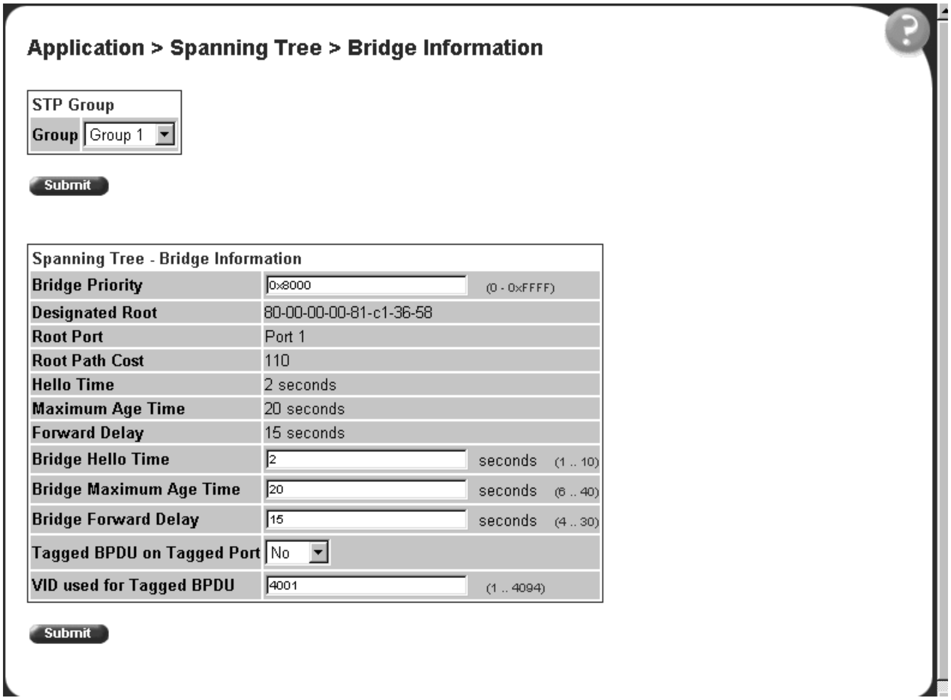
You can view and configure existing Spanning Tree switch settings.

To configure Spanning Tree switch settings:

1 From the main menu, choose Application > Spanning Tree > Bridge Information.

The Spanning Tree Bridge Information page opens (Figure 90).

Figure 90 Spanning Tree Bridge Information page



STP Group

Group	Group 1

Spanning Tree - Bridge Information

Bridge Priority	0x8000		(0 - 0xFFFF)
Designated Root	80-00-00-00-81-c1-36-58		
Root Port	Port 1		
Root Path Cost	110		
Hello Time	2 seconds		
Maximum Age Time	20 seconds		
Forward Delay	15 seconds		
Bridge Hello Time	2	seconds	(1 .. 10)
Bridge Maximum Age Time	20	seconds	(6 .. 40)
Bridge Forward Delay	15	seconds	(4 .. 30)
Tagged BPDU on Tagged Port	No		
VID used for Tagged BPDU	4001		(1 .. 4094)

Table 74 describes the items on the Spanning Tree Bridge Information page.

Table 74 Spanning Tree Bridge Information page items

Section	Item	Range	Description
STP Group	Group		Choose the STP Group you want to work with.
Spanning Tree - Bridge Information	Bridge Priority	0..65535	Type the priority value of the bridge ID in hexadecimal notation, which is the most significant byte of the bridge ID. The Spanning Tree Algorithm uses this parameter to determine the root bridge (or designated bridge). For example, the bridge with the lowest bridge ID becomes the root bridge, with Bridge Priority values compared first, followed by the hardware addresses. The default setting is 8000.
	Designated Root	XXXXXXX XXXXXXX	The bridge ID of the root bridge, as determined by the Spanning Tree Algorithm.
	Root Port	1..28	The port number of the port which offers the lowest cost past from this bridge to the root bridge.
	Root Path Cost	Integer	The cost of the path to the root as seen from this bridge.
	Hello Time	1..10 seconds	The actual Hello Interval, the amount of time between transmissions of configuration Bridge Protocol Data Units (BPDUs) that the root bridge is currently using. Note: Bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. See also Bridge Hello Time.
	Maximum Age Time	6..40 seconds	The Maximum Age Time parameter value that the root bridge is currently using. This value specifies the maximum age that a Hello message can attain before it is discarded. Note: The root bridge's Maximum Age Time parameter value becomes the actual Maximum Age Time parameter value for all bridges participating in the spanning tree network. See also Bridge Maximum Age Time.
	Forward Delay	4..30 seconds	The Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note: The root bridge's Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network. See also Bridge Forward Delay.

Table 74 Spanning Tree Bridge Information page items

Section	Item	Range	Description
	Bridge Hello Time	1..10 seconds	The Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note: Although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. See also Hello Time. The default setting is 2 seconds.
	Forward Delay	4..30 seconds	The Forward Delay parameter value that the root bridge is currently using. This value specifies the amount of time that the bridge ports remain in the Listening and Learning states before entering the Forwarding state. Note: The root bridge's Forward Delay parameter value becomes the actual Forward Delay parameter value for all bridges participating in the spanning tree network. See also Bridge Forward Delay.
	Bridge Hello Time	1..10 seconds	The Hello Interval (the amount of time between transmissions of BPDUs) specified by management for this bridge. This parameter takes effect only when this bridge becomes the root bridge. Note: Although you can set the Hello Interval for a bridge using bridge management software, once the spanning tree computation process is complete, all bridges participating in the spanning tree network use the root bridge's Hello Interval parameter value. If any bridge becomes the root bridge, its Hello Interval parameter value becomes the Actual Hello Interval parameter value for all bridges participating in the spanning tree network. See also Hello Time. The default setting is 2 seconds.
	Tagged BPDU on Tagged Port	(1) Yes (2) No	Displays whether you are sendin]g either tagged or untagged BPDUs from a tagged port.
	VID used for Tagged BPDU	1-4094	Displays the VLAN ID you are sending the tagged BPDUs for the specified STG to.

2 Type information in the text boxes, or select from a list.

3 Click Submit.

Configuring MultiLink Trunk (MLT) members

You can configure groups of links between the BPS 2000 and another switch or a server to provide higher bandwidth with active redundant links. Trunked ports can span multiple units of the stack for fail-safe connectivity to mission-critical servers and the network center.

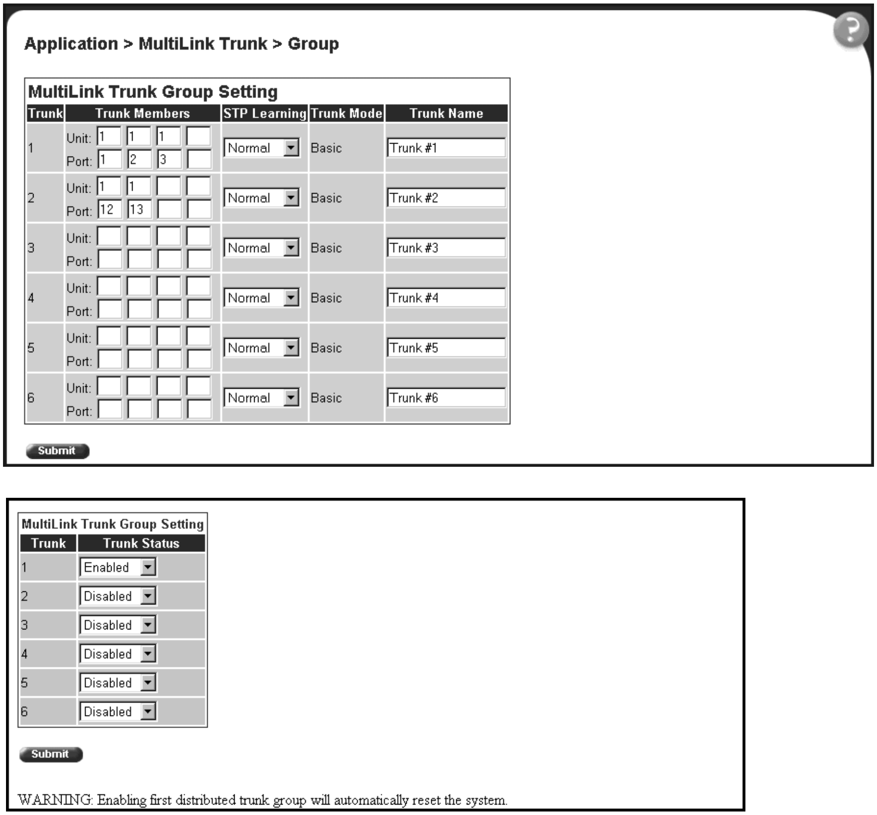
You can configure two to four switch ports together as members of a trunk to a maximum of six trunks.

To configure MultiLink Trunk members:

1. From the main menu, choose Application > MultiLink Trunk > Group.

   The Group page opens (Figure 91).

Figure 91 Group page



Application > MultiLink Trunk > Group

MultiLink Trunk Group Setting

Trunk	Trunk Members	STP Learning	Trunk Mode	Trunk Name
1	Unit: 1 1 1 Port: 1 2 3	Normal	Basic	Trunk #1
2	Unit: 1 1 Port: 12 13	Normal	Basic	Trunk #2
3	Unit: Port:	Normal	Basic	Trunk #3
4	Unit: Port:	Normal	Basic	Trunk #4
5	Unit: Port:	Normal	Basic	Trunk #5
6	Unit: Port:	Normal	Basic	Trunk #6

MultiLink Trunk Group Setting

Trunk	Trunk Status
1	Enabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled

WARNING: Enabling first distributed trunk group will automatically reset the system.

Table 75 describes the items on the Group page.

Table 75 Group page items

Section	Item	Range	Description
MultiLink Trunk Group Setting	Trunk	1..6	This column contains fields in each row that can be configured to create the corresponding trunk. The Unit value in the (Unit/Port) field is configurable only when the switch (unit) is part of a stack configuration. It indicates that the trunk members in this row are associated with the specified unit number configured in the Unit field. Each switch port can only be a member of a single trunk. The appropriate trunk number for each trunk member configured within this field is shown adjacent to the corresponding switch port on the following management pages: Port Configuration (see Figure 43 on page 112) and Spanning Tree Configuration (see Figure 83 on page 189). There are no default settings.
	Trunk Port Members	Unit: 1..8 Port: 1..28	Type the switch and port numbers to associate with the corresponding trunk. Note: You can configure two to four switch ports together as members of a trunk to a maximum of six trunks. Switch ports can only be assigned a member of a single trunk. There are no default settings.
	STP Learning	(1) Normal (2) Fast (3) Disabled	Choose the parameter that allows the specified trunk to participate in the spanning tree. This setting overrides those of the individual trunk members. Selecting Fast shortens the state transition timer by two seconds. The default setting is Normal.
	Trunk Mode	Basic	The default operating mode of the switch. When in Basic mode, source MAC addresses are dynamically assigned to specific trunk members for flooding and forwarding. This allows the switch to stabilize and distribute the data streams of source addresses across the trunk members.
	Trunk Name	1..20	Type a character string to create a unique name to identify the trunk, for example, Trunk1. The name, if chosen carefully, can provide meaningful information to you. For example, S1:T1 to FS2 indicates that Trunk1, in Switch1 connects to File Server 2.
MultiLink Trunk Group Setting	Trunk Status	(1) Enabled (2) Disabled	Choose to enable or disable any of the existing MultiLink Trunks. Note: When a trunk is not active (Trunk Status field set to Disabled), configuration changes do not take effect until you set the Trunk Status field to enabled.

2 Type information in the text boxes, or select from a list.

3 Click Submit in any section to save your changes.

Monitoring MLT traffic

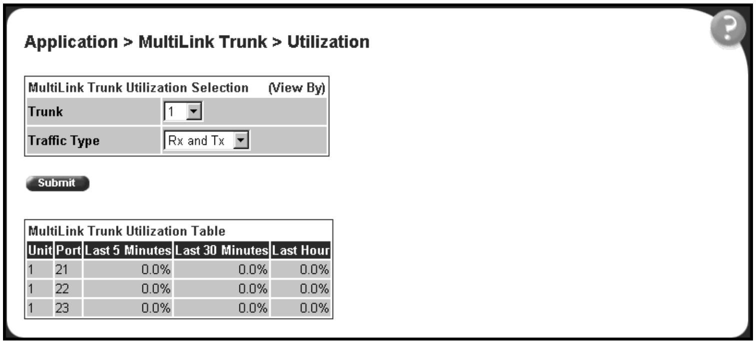
You can monitor the bandwidth usage for the MultiLink Trunk member ports within each trunk in your configuration by selecting the traffic type to monitor.

To monitor MultiLink Trunk traffic:

1 From the main menu, choose Application > MultiLink Trunk > Utilization.

The Utilization page opens (Figure 92).

Figure 92 Utilization page



Application > MultiLink Trunk > Utilization

MultiLink Trunk Utilization Selection (View By)	
Trunk	1
Traffic Type	Rx and Tx

MultiLink Trunk Utilization Table

Unit	Port	Last 5 Minutes	Last 30 Minutes	Last Hour
1	21	0.0%	0.0%	0.0%
1	22	0.0%	0.0%	0.0%
1	23	0.0%	0.0%	0.0%

Table 76 describes the items on the Utilization page.

Table 76 Utilization page items

Section	Item	Range	Description
MultiLink Trunk Utilization Selection (View By)	Trunk	1..6	Choose the trunk to be monitored.
	Traffic Type	(1) RX and TX (2) RX (3) TX	Choose the traffic type to be monitored for percentage of bandwidth utilization.

Table 76 Utilization page items (continued)

Section	**Item**	**Range**	**Description**
MultiLink Trunk Utilization Table	Unit/Port		A list of the trunk member switch ports that correspond to the trunk specified in the Trunk column.
	Last 5 Minutes%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last five minutes. This field provides a running average of network activity, and is updated every 15 seconds.
	Last 30 Minutes%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 30 minutes. This field provides a running average of network activity, and is updated every 15 seconds.
	Last Hour%		The percentage of packets (of the type specified in the Traffic Type field) used by the port in the last 60 minutes. This field provides a running average of network activity, and is updated every 15 seconds.

2 In the MultiLink Trunk Utilization Selection section, type the Trunk number and traffic type to be monitored.

3 Click Submit.

The results of your request are displayed in the MultiLink Trunk Utilization Table (Figure 92).

Chapter 8
Implementing QoS Using QoS Wizard and QoS Quick Config

You can configure Quality of Service (QoS) features in your network by using the Web-based QoS Wizard, using the QoS Quick Config pages, or using the Advanced QoS configuration pages available in the Web-based management user interface.

This chapter shows how to use the QoS Wizard and QoS Quick Config pages to configure QoS parameters for the BPS 2000. (Refer to Chapter 9 for information on configuring QoS using the Advanced QoS Web pages.)

This chapter covers the following topics:

- "Using QoS Wizard," next
- "Using QoS Quick Config" on page 236

Note: To configure the features introduced with software version 1.2 and higher in a mixed stack, you must access a BPS 2000 unit.

Using QoS Wizard

The QoS Wizard provides a set of Web pages that allows you to specify common QoS settings for the BPS 2000.

Warning: Nortel Networks recommends that you use the QoS Wizard for your *initial* configuration only. Each time the QoS Wizard is initiated, all existing configurations are reset to the default values. After you complete the *initial* QoS Wizard configuration method, you can then customize traffic treatment using the QoS Advanced configuration process.

This section discusses the following topics:

- "Configuring Standard traffic with the QoS Wizard" on page 208
- "Prioritizing traffic with the QoS Wizard" on page 210
- "Prioritizing VLANs with the QoS Wizard" on page 213
- "Prioritizing IP applications with the QoS Wizard" on page 220
- "Prioritizing user defined flows with the QoS Wizard" on page 226

Note: All the settings you configure with QoS Wizard are actually set when you click the final Finish and see the Session Confirmation page.

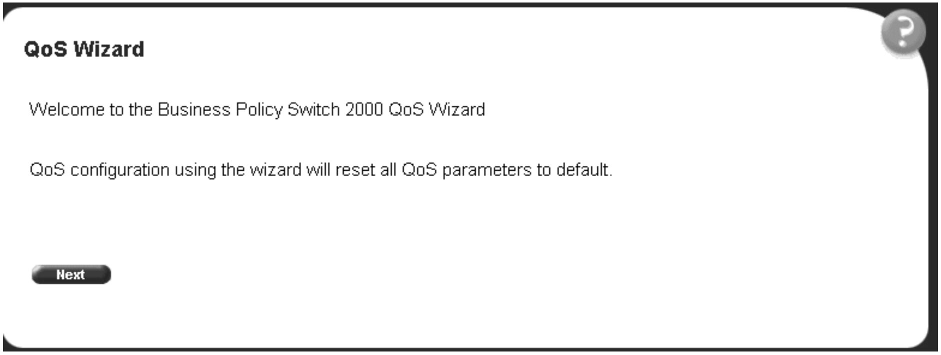
Configuring Standard traffic with the QoS Wizard

To use the QoS Wizard to configure Standard traffic:

1 From the main menu, choose Application > QoS > QoS Wizard.

The QoS Wizard opens (Figure 93).

Figure 93 QoS Wizard opening page



QoS Wizard

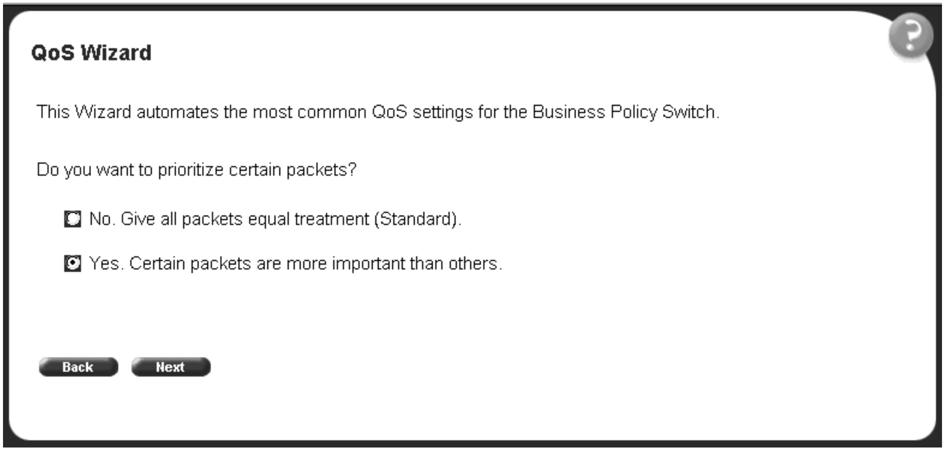
Welcome to the Business Policy Switch 2000 QoS Wizard

QoS configuration using the wizard will reset all QoS parameters to default.

2 To continue the configuration process, click Next.

A packet prioritization selection page opens (Figure 94).

Figure 94 Packet prioritization selection page



QoS Wizard

This Wizard automates the most common QoS settings for the Business Policy Switch.

Do you want to prioritize certain packets?

○ No. Give all packets equal treatment (Standard).

● Yes. Certain packets are more important than others.

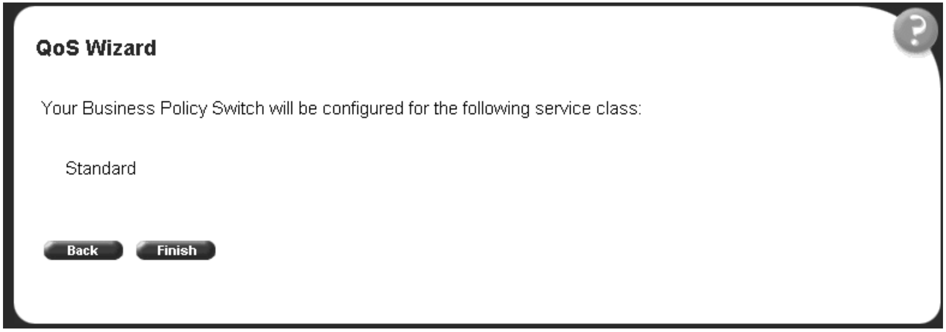
3 Select No.

4 Click Next.

A Standard prioritization page opens (Figure 95).

Note: If you want to prioritize traffic, skip this step and continue the steps outlined in "Prioritizing traffic with the QoS Wizard."

Figure 95 Standard prioritization page



QoS Wizard

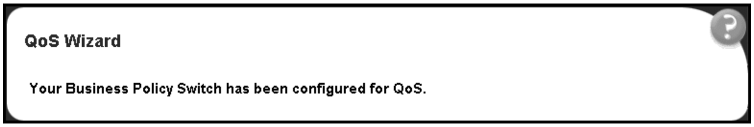
Your Business Policy Switch will be configured for the following service class:

Standard

5 To complete the configuration process, click Finish.

The session confirmation page appears (Figure 96).

Figure 96 Session confirmation page



QoS Wizard

Your Business Policy Switch has been configured for QoS.

Prioritizing traffic with the QoS Wizard

You can specify that different types of traffic in your network configuration be marked with different priority levels.

The QoS Wizard allows you to prioritize traffic flows by:

- VLAN
- IP application
- User defined flow

Using the QoS Wizard, you can prioritize traffic by one of these categories, by two categories, or by all three. Also, you can define more than one flow in each category. The QoS Wizard leads you through the following four general steps in defining each flow you want to prioritize:

- Step 1 is setting the category of prioritized traffic flow—VLAN, IP Application, or User defined flow.

  The User defined flow has two steps in classifying the flow:

  - Policy Label
  - Policy Definition
- Step 2/3 is setting a Meter for the flow, if you want
- Step 3/4 is choosing the Service Class or Drop for the flow

  If you are metering traffic within the flow, you choose two separate Service Classes: one for In-Profile traffic, and one for Out-of-Profile traffic. If you are not metering traffic within the flow, you choose only one Service Class.
- Step 4/5 is setting a Shaper, or shaping criteria, for the flow, if you want

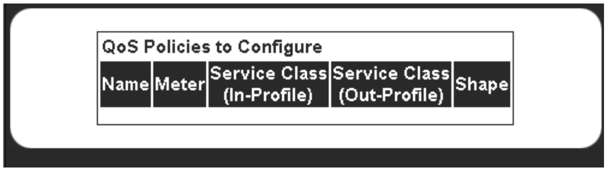
Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

The QoS Wizard automatically steps you through each of these four steps for each flow you want to prioritize. You can prioritize flows within three different categories and more than one flow per category. When you fill the resources of one category, you will not be prompted again, and you see a check mark next to that category if there are some flows to be configured or an X mark next to that category if there are no flows to be configured in the packet prioritization screen (Figure 98). You will be unable to configure more flows for that category. Should you fill the QoS Wizard resources, you will not be prompted again.The QoS Wizard automatically presents screens to configure each prioritized traffic flow.

Additionally, the packet prioritization screen has a Status button that displays a QoS Policies to Configure in a pop-up window (Figure 97). As you finish configuring each type of flow, this pop-up window displays with the configured flows you configure using the QoS Wizard listed. When you completely finish the QoS Wizard, the policies are implemented.

Note: The system configures the QoS parameters you configure using the QoS Wizard only when you click Finish.

Figure 97 QoS Policies to Configure window



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape

The QoS Policies to Configure table has the following fields:

— Name—Displays the name of the policy.

— Meter—Displays whether you are metering the data in the flow associated with the policy.

— Service Class (In-Profile)—Displays the service class of the flow associated with the policy. If you are metering the data, this is the service class for the data that fits the metered profile.

— Service Class (Out-Profile)—Displays the service class of metered data that falls outside the profile.

— Shape—Displays whether you are shaping the data in the flow associated with the policy.

To assign priority levels to different types of network traffic:

1 From the main menu, choose Application > QoS > QoS Wizard.

The QoS Wizard opens (Figure 93).

2 To continue the configuration process, click Next.

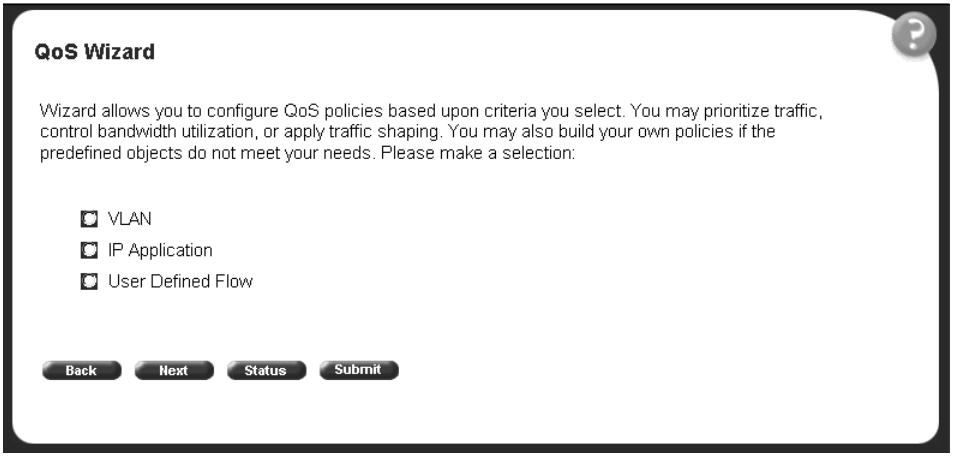
A packet prioritization selection page opens (Figure 94).

3 Select Yes.

4 Click Next.

A packet prioritization explanation page opens (Figure 98).

Figure 98 Packet prioritization explanation page



Wizard allows you to configure QoS policies based upon criteria you select. You may prioritize traffic, control bandwidth utilization, or apply traffic shaping. You may also build your own policies if the predefined objects do not meet your needs. Please make a selection:

☐ VLAN
☐ IP Application
☐ User Defined Flow

a To see the policies you have configured, click Status.

The QoS Policies to Configure table opens in a pop-up window (Figure 97).

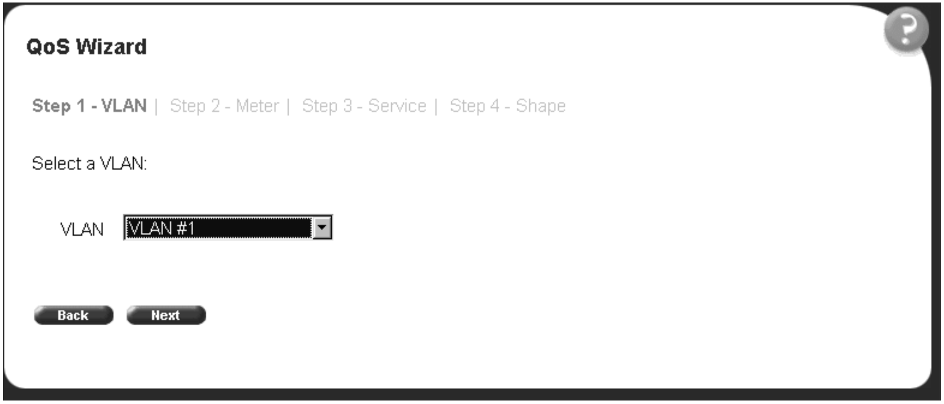
Prioritizing VLANs with the QoS Wizard

You can specify that different VLANs in your network configuration be marked with different priority levels.

1 In the packet prioritization window (Figure 98), click VLAN, and click Next.

A VLAN prioritization selection page opens (Figure 99).

Figure 99 VLAN prioritization selection page



QoS Wizard

Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

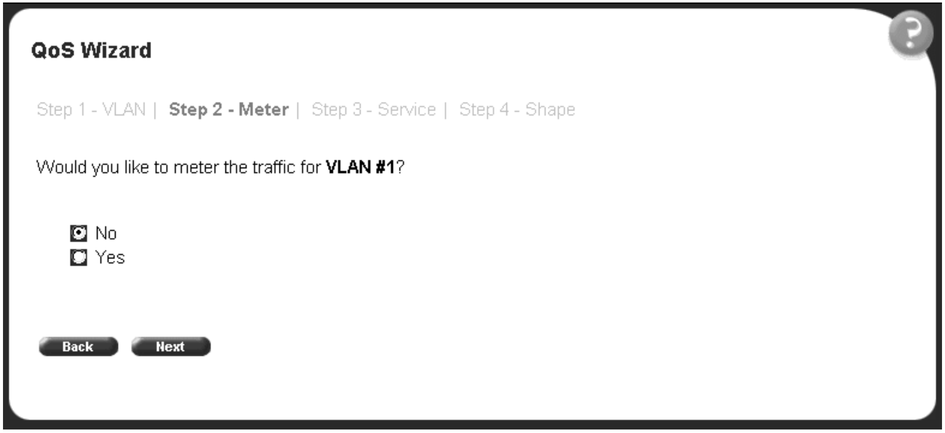
Select a VLAN:

VLAN: VLAN #1

2 Choose the VLAN and click Next.

A page opens (Figure 100) that asks if you want to set a Meter for the specified VLAN.

Figure 100 Meter for VLAN page



QoS Wizard

Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

Would you like to meter the traffic for **VLAN #1**?

● No
○ Yes

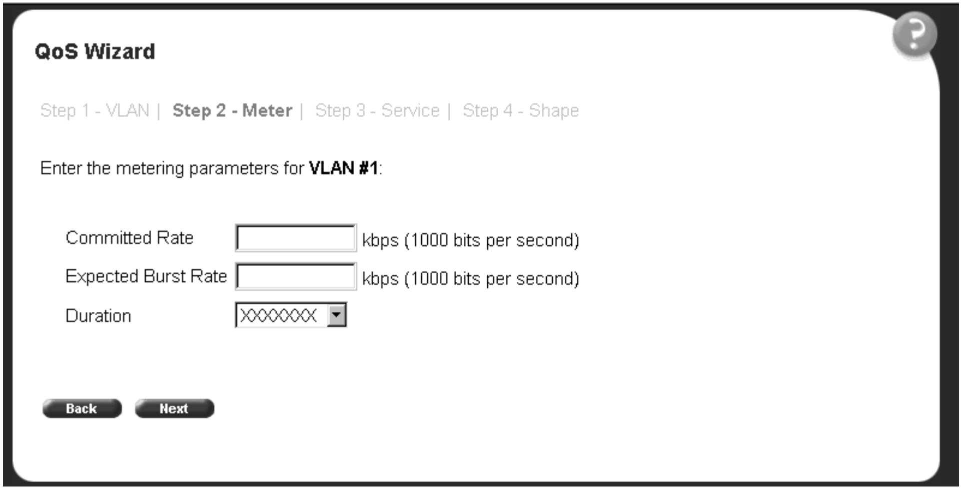
3 If you do not want to set a Meter, click No.

The system opens to the Service Class selection page (Figure 102), which appears with only one Service Class to set. You do not have In-Profile and Out-of-Profile without metering data.

4 If you want to set a Meter, click Yes.

A page opens (Figure 101) that allows you to set a Meter for the specified VLAN.

Figure 101 Meter setting for VLAN page



QoS Wizard

Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

Enter the metering parameters for **VLAN #1**:

Committed Rate ☐ kbps (1000 bits per second)

Expected Burst Rate ☐ kbps (1000 bits per second)

Duration XXXXXXX

5 Enter the committed rate you want for this Meter.

6 Enter the expected burst rate you want for this Meter.

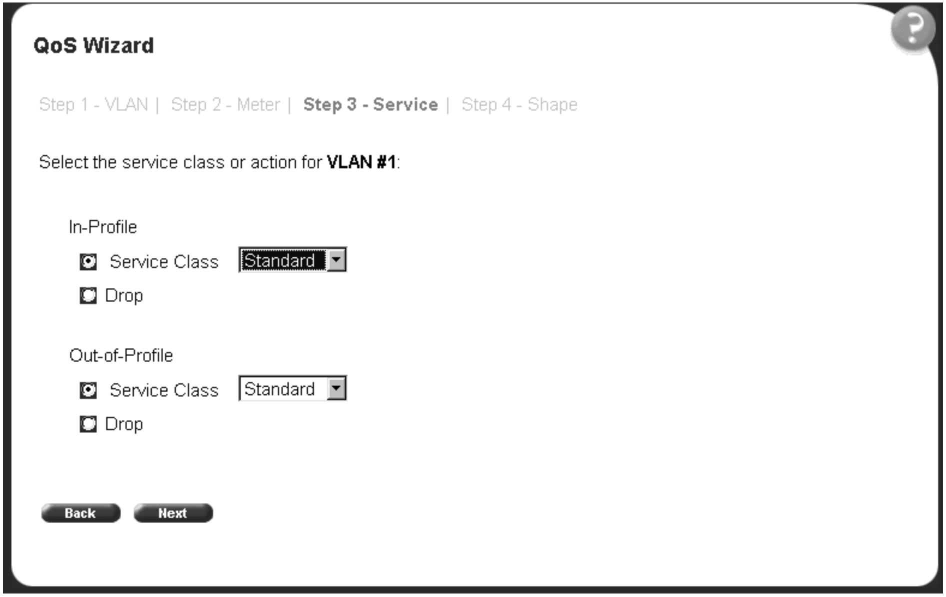
The system calculates a series of 7 or fewer possible durations for the committed and expected burst rates you set.

7 Choose the Duration you want.

8 Click Next.

A page opens (Figure 102) that allows you to select a Service Class separately for both the In-Profile and Out-of-Profile Action for the specified VLAN.

Figure 102 Service Class selection for VLAN page



QoS Wizard

Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

Select the service class or action for **VLAN #1**:

In-Profile

● Service Class: Standard

○ Drop

Out-of-Profile

● Service Class: Standard

○ Drop

9 Click either Service Class or Drop.

If you click Service Class, choose the Service Class you want from the pull-down menu.

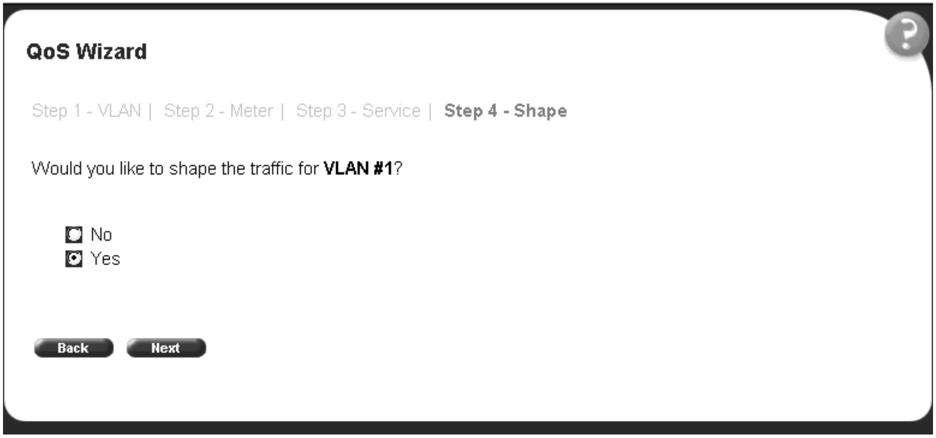
If you click Drop, the traffic in the specified VLAN is dropped.

10 Click Next.

A page opens (Figure 103) that allows you to set shaping criteria for the specified VLAN.

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

Figure 103 Shaper for VLAN page


QoS Wizard
Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | Step 4 - Shape
Back
Next

Would you like to shape the traffic for **VLAN #1**?

☐ No
☑ Yes

11 If you do not want to shape traffic for the specified VLAN, click No.

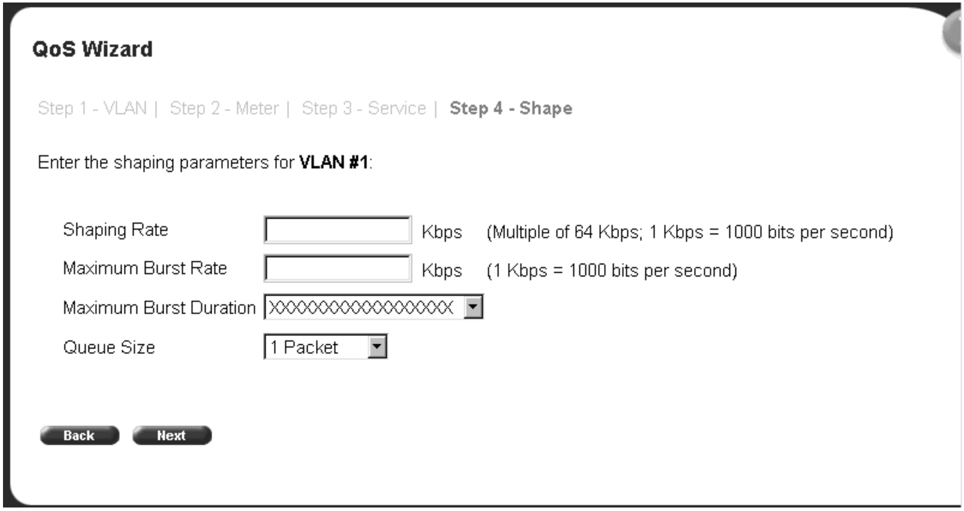
The system opens to a page (Figure 105) that asks you if you want to prioritize traffic for another VLAN.

If you fill the resources of the QoS Wizard, you will not be prompted for another VLAN.

12 If you want to shape traffic for the specified VLAN, click Yes.

A page opens (Figure 104) that allows you to set shaping parameters for the specified VLAN.

Figure 104 Setting shaping parameters for VLAN page



QoS Wizard

Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | **Step 4 - Shape**

Enter the shaping parameters for **VLAN #1**:

Shaping Rate Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)

Maximum Burst Rate Kbps (1 Kbps = 1000 bits per second)

Maximum Burst Duration XXXXXXXXXXXXXXXXXX

Queue Size 1 Packet

13 Enter the shaping rate you want for this Shaper.

The system rounds up shaping rates you enter, including 0, to multiples of 64 Kbps.

14 Enter the maximum burst rate you want for this Shaper.

The system calculates a series of 6 or fewer possible durations for the shaping and maximum burst rates you set.

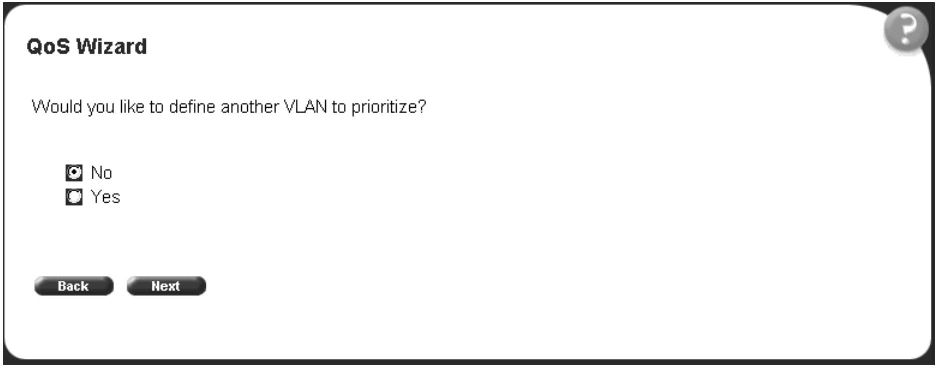
15 Choose the Maximum Burst Duration from the pull-down menu.

16 Choose the queue size you want for this Shaper.

17 Click Next.

A page opens (Figure 105) that asks you if you want to prioritize traffic for another VLAN. If you fill the resources of the QoS Wizard, you will not be prompted for another VLAN.

Figure 105 Additional VLANs page



QoS Wizard

Would you like to define another VLAN to prioritize?

● No
○ Yes

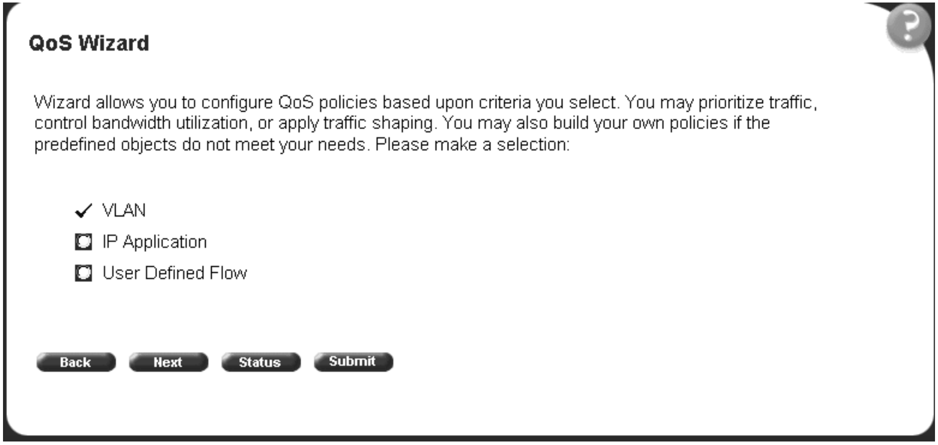
18 If you want to prioritize traffic for another VLAN, click Yes and Next.

The system returns you to the VLAN prioritization page (Figure 99), and you continue through steps 1 to 17 for the next VLAN.

19 If you do not want to prioritize traffic for another VLAN, click No and Next.

The system returns you to the packet prioritization page (Figure 106), with a check mark next to VLAN,. If you click Status, the QoS Policies to Configure table listing your new entry simultaneously appears in a pop-up window (Figure 107).

Figure 106 Packet prioritization page with prioritized VLAN(s)

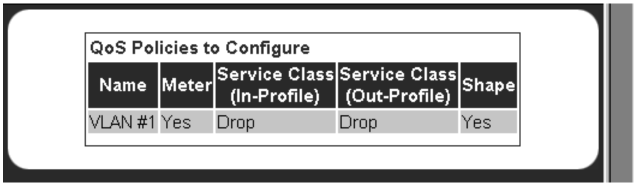


QoS Wizard

Wizard allows you to configure QoS policies based upon criteria you select. You may prioritize traffic, control bandwidth utilization, or apply traffic shaping. You may also build your own policies if the predefined objects do not meet your needs. Please make a selection:

✓ VLAN
☐ IP Application
☐ User Defined Flow

Figure 107 QoS Policies to Configure window with VLAN entry



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape
VLAN #1	Yes	Drop	Drop	Yes

20 When you are through with the table, click Back, then click Submit.

You will see a session confirmation page.

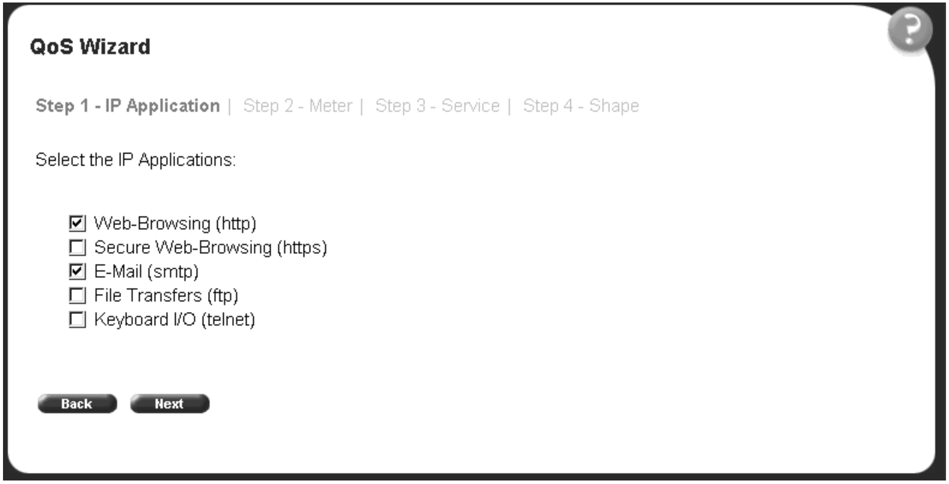
Prioritizing IP applications with the QoS Wizard

You can specify that different IP applications in your network configuration are marked with different priority levels.

1 In the packet prioritization window (Figure 98), click IP Application, and click Next.

An IP Application prioritization selection page opens (Figure 108).

Figure 108 IP Application prioritization page



QoS Wizard

Step 1 - IP Application | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

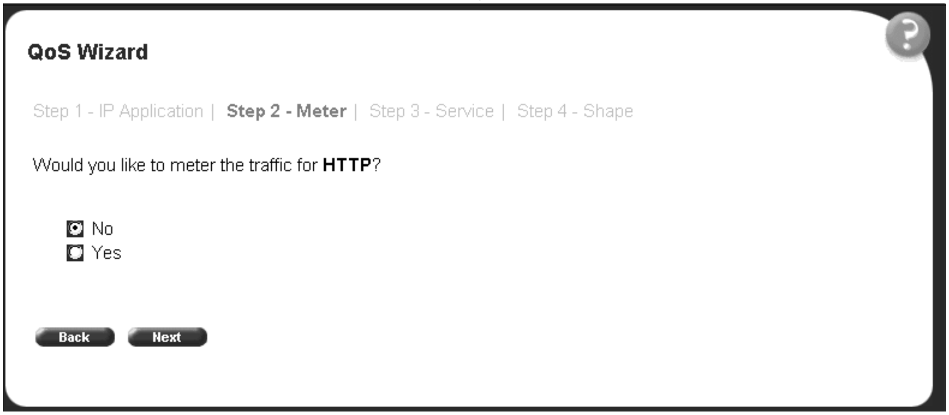
Select the IP Applications:

- ☑ Web-Browsing (http)
- ☐ Secure Web-Browsing (https)
- ☑ E-Mail (smtp)
- ☐ File Transfers (ftp)
- ☐ Keyboard I/O (telnet)

2 Click the application(s) you want to prioritize and click Next.

A page opens (Figure 109) that asks if you want to set a Meter for the specified IP Application.

Figure 109 Meter for IP Application page



QoS Wizard

Step 1 - IP Application | **Step 2 - Meter** | Step 3 - Service | Step 4 - Shape

Would you like to meter the traffic for **HTTP**?

- ● No
- ○ Yes

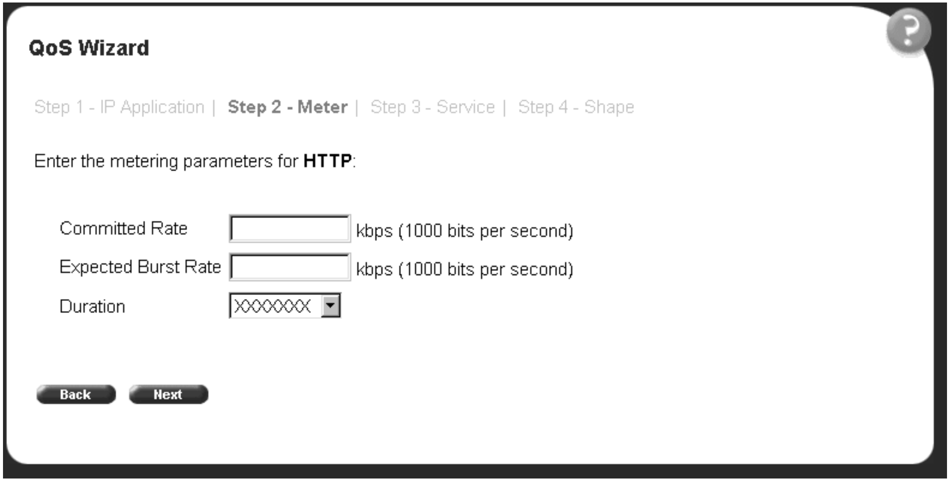
3 If you do not want to set a Meter, click No.

The system opens to the Service Class selection page (Figure 111), which appears with only one Service Class to set. You do not have In-Profile and Out-of-Profile without metering data.

4 If you want to set a Meter, click Yes.

A page opens (Figure 110) that allows you to set a Meter for the specified IP Application.

Figure 110 Meter setting for IP Application page



QoS Wizard

Step 1 - IP Application | **Step 2 - Meter** | Step 3 - Service | Step 4 - Shape

Enter the metering parameters for **HTTP**:

Committed Rate		kbps (1000 bits per second)
Expected Burst Rate		kbps (1000 bits per second)
Duration	XXXXXXX	

5 Enter the committed rate you want for this Meter.

6 Enter the expected burst rate you want for this Meter.

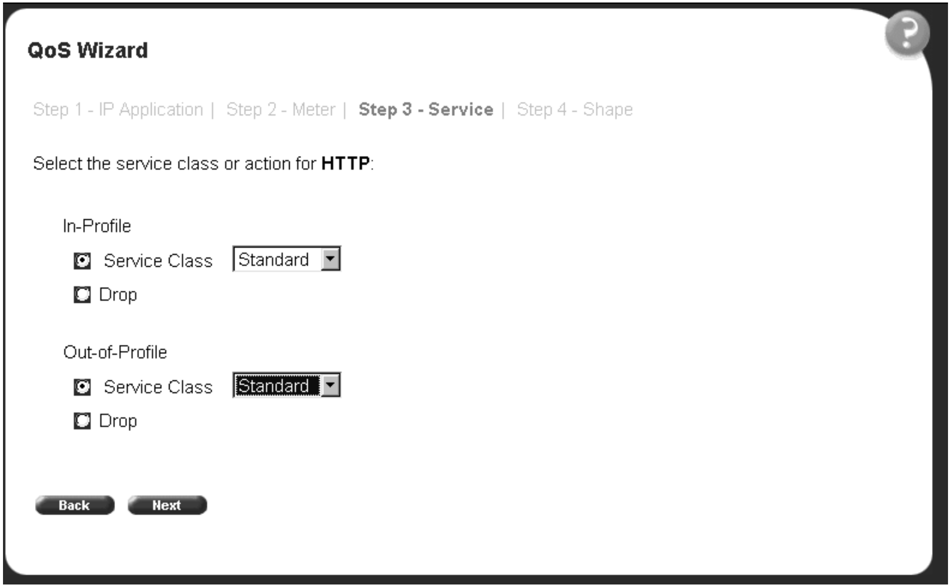
The system calculates a series of 7 or fewer possible durations for the committed and expected burst rates you set.

7 Choose the Duration you want.

8 Click Next.

A page opens (Figure 111) that allows you to select a Service Class separately for both the In-Profile and Out-of-Profile Action for the specified IP Application.

Figure 111 Service Class selection for IP Application page


QoS Wizard
Step 1 - IP Application | Step 2 - Meter | Step 3 - Service | Step 4 - Shape
Back
Next

Select the service class or action for **HTTP**:

In-Profile

● Service Class: Standard

○ Drop

Out-of-Profile

● Service Class: Standard

○ Drop

9 Click either Service Class or Drop.

If you click Service Class, choose the Service Class you want from the pull-down menu.

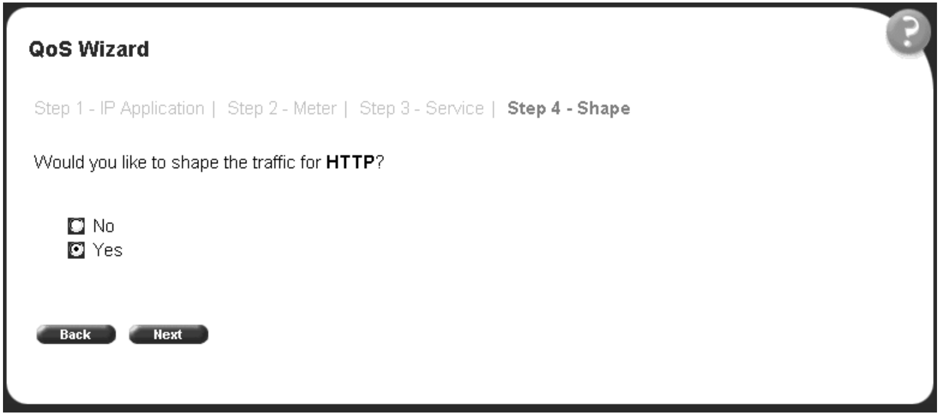
If you click Drop, the traffic in the specified IP Application is dropped.

10 Click Next.

A page opens (Figure 112) that allows you to set shaping criteria for the specified IP Application.

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

Figure 112 Shaper for IP Application page



QoS Wizard

Step 1 - IP Application | Step 2 - Meter | Step 3 - Service | Step 4 - Shape

Would you like to shape the traffic for **HTTP**?

○ No
● Yes

11 If you do not want to shape traffic for the specified IP Application, click No.

a If you chose more than one IP Application to prioritize, a page opens that asks if you want to set a Meter for the next specified IP Application (Figure 109). Repeat steps 3 through 17 for each IP Application you chose.

b If you chose just one IP Application, you have completed the QoS Wizard prioritization process for that flow. Go to The system returns you to the packet prioritization page (Figure 114), with a check mark next to IP Application,

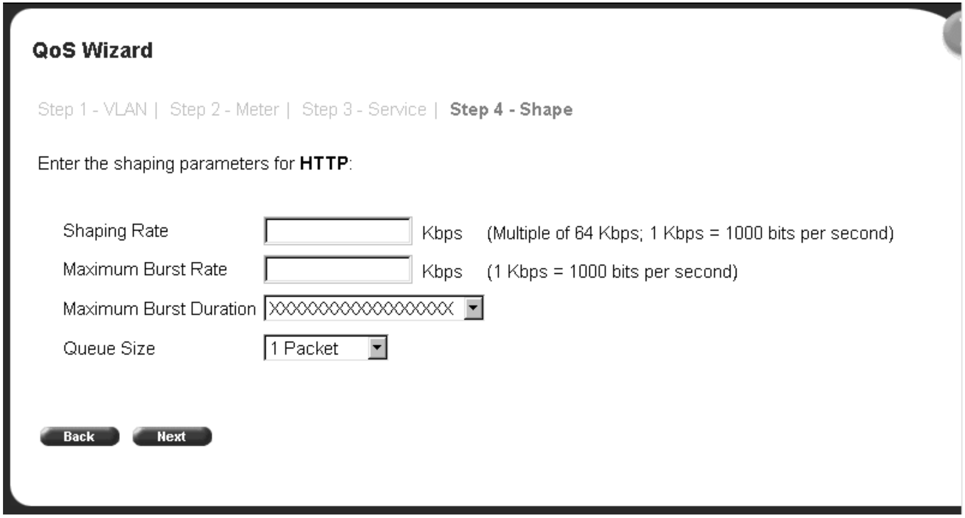
If you fill the resources of the QoS Wizard, you will not be prompted for another IP Application.

If you click Status, the QoS Policies to Configure table listing your new entry simultaneously appears in a pop-up window (Figure 115).

12 If you want to shape traffic for the specified IP Application, click Yes.

A page opens (Figure 113) that allows you to set shaping parameters for the specified IP Application.

Figure 113 Setting shaping parameters for IP Application page



QoS Wizard

Step 1 - VLAN | Step 2 - Meter | Step 3 - Service | **Step 4 - Shape**

Enter the shaping parameters for **HTTP**:

Shaping Rate Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)

Maximum Burst Rate Kbps (1 Kbps = 1000 bits per second)

Maximum Burst Duration XXXXXXXXXXXXXXXXX

Queue Size 1 Packet

13 Enter the shaping rate you want for this Shaper.

The system rounds up shaping rates you enter, including 0, to multiples of 64 Kbps.

14 Enter the maximum burst rate you want for this Shaper.

The system calculates a series of 6 or fewer possible durations for the shaping and maximum burst rates you set.

15 Choose the Maximum Burst Duration from the pull-down menu.

16 Choose the queue size you want for this Shaper.

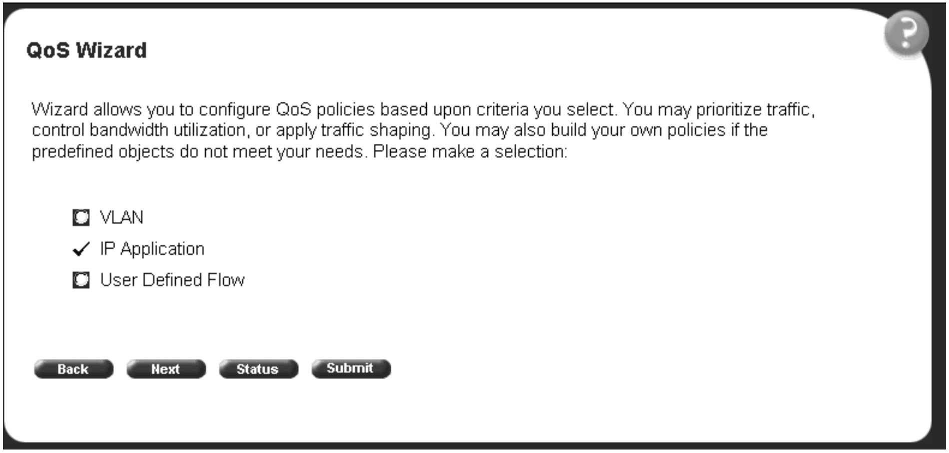
17 Click Next.

a If you chose more than one IP Application to prioritize, a page opens that asks if you want to set a Meter for the next specified IP Application (Figure 109). Repeat steps 3 through 17 for each IP Application you chose.

b If you chose just one IP Application, you have completed the QoS Wizard prioritization process for that flow. The system returns you to the packet prioritization page (Figure 114), with a check mark next to IP Application. Press the Status button to view the QoS Policies to Configure table listing your new entry in a pop-up window (Figure 115).

If you fill the resources of the QoS Wizard, you will not be prompted for another IP Application.

Figure 114 Packet prioritization page with prioritized IP Application(s)

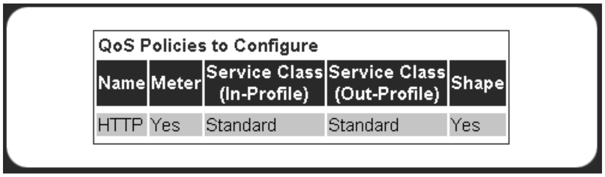


QoS Wizard

Wizard allows you to configure QoS policies based upon criteria you select. You may prioritize traffic, control bandwidth utilization, or apply traffic shaping. You may also build your own policies if the predefined objects do not meet your needs. Please make a selection:

☐ VLAN
✓ IP Application
☐ User Defined Flow

Figure 115 QoS Policies to Configure window with IP Application entry



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape
HTTP	Yes	Standard	Standard	Yes

18 When you are through viewing the table, click Back, then Submit.

You see a session confirmation page.

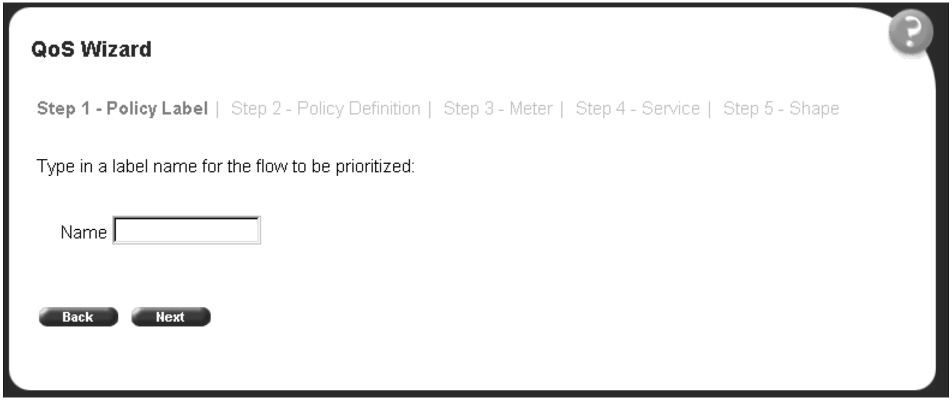
Prioritizing user defined flows with the QoS Wizard

You can specify that different user defined flows in your network configuration be marked with different priority levels.

1 In the packet prioritization window (Figure 98), click User Defined Flow, and click Next.

A page opens (Figure 116) that asks the user to assign a name to the flow.

Figure 116 Policy label page

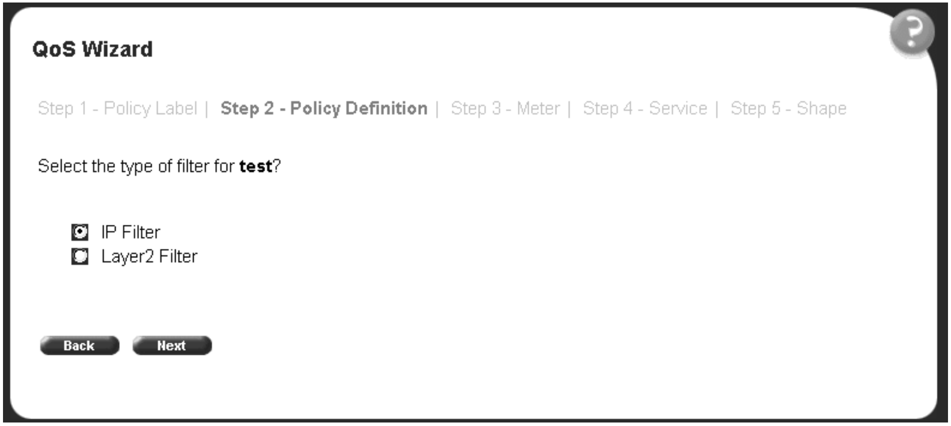

QoS Wizard
Step 1 - Policy Label | Step 2 - Policy Definition | Step 3 - Meter | Step 4 - Service | Step 5 - Shape
Name
Back
Next

Type in a label name for the flow to be prioritized:

2 Enter the name of the flow and click Next.

A page opens (Figure 117) that asks if you want to set an IP filter or a layer 2 filter.

Figure 117 Policy definition page


QoS Wizard
Step 1 - Policy Label | Step 2 - Policy Definition | Step 3 - Meter | Step 4 - Service | Step 5 - Shape
Back
Next

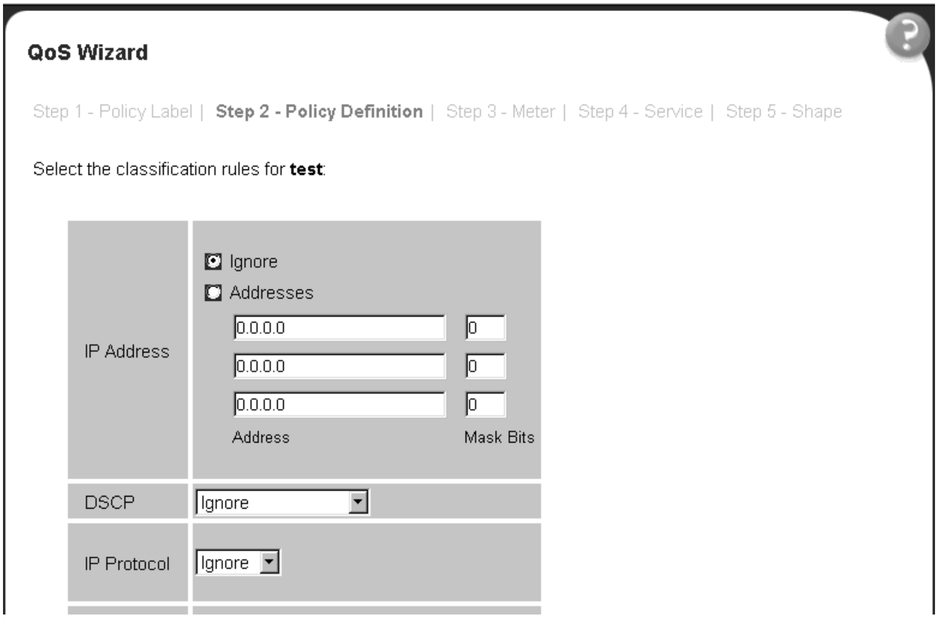
Select the type of filter for **test**?

● IP Filter
○ Layer2 Filter

a If you want an IP filter, click IP Filter and click Next.

A page opens that requests the customer to choose the IP filter criteria for the specified flow (Figure 118 and Figure 119).

Figure 118 IP classification rules page (1 of 2)



QoS Wizard

Step 1 - Policy Label | **Step 2 - Policy Definition** | Step 3 - Meter | Step 4 - Service | Step 5 - Shape

Select the classification rules for **test**:

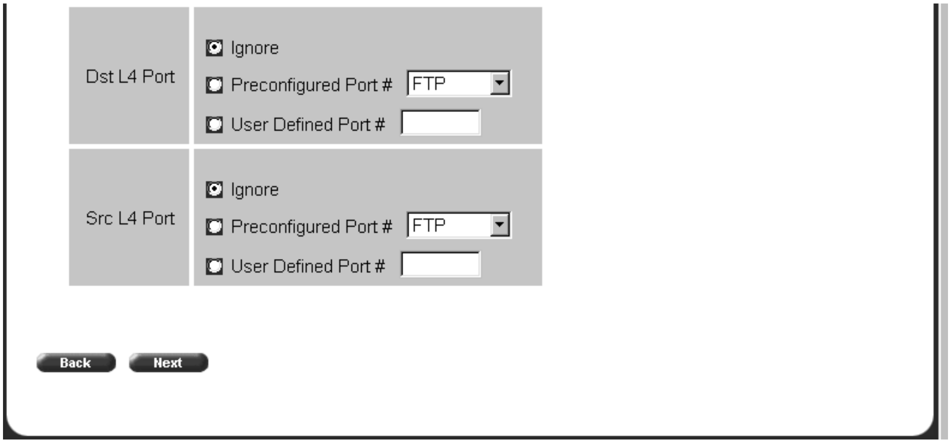
IP Address
● Ignore
○ Addresses

Address	Mask Bits
0.0.0.0	0
0.0.0.0	0
0.0.0.0	0

DSCP: Ignore

IP Protocol: Ignore

Figure 119 IP classification rules page (2 of 2)



Dst L4 Port
● Ignore
○ Preconfigured Port #: FTP
○ User Defined Port #:

Src L4 Port
● Ignore
○ Preconfigured Port #: FTP
○ User Defined Port #:

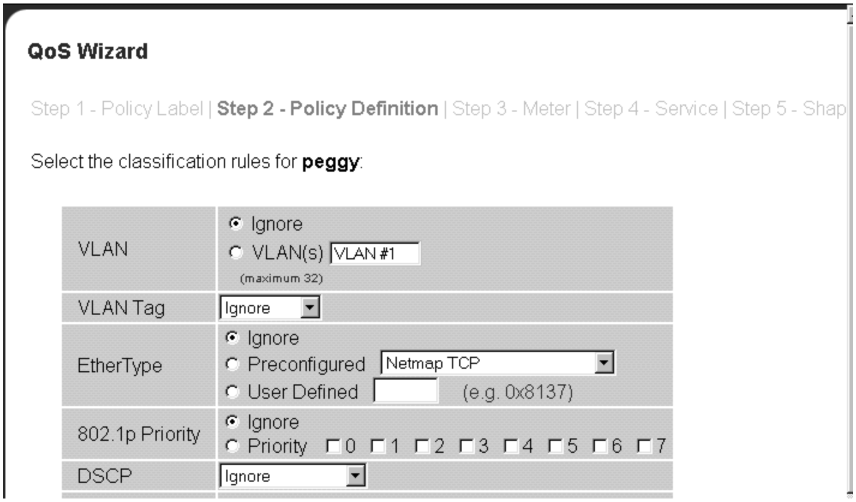
- — Choose the IP filter parameters you want the flow to have. (Refer to Chapter 9 for a description of the parameters.)
- — Click Next.

A page opens (Figure 122) that asks if you want to set a Meter for the specified flow.

b If you want a layer 2 filter, click Layer2 Filter and click Next.

A page opens that requests the customer to choose the layer 2 filter criteria for the specified flow (Figure 120 and Figure 121).

Figure 120 Layer 2 classification rules page (1 of 2)



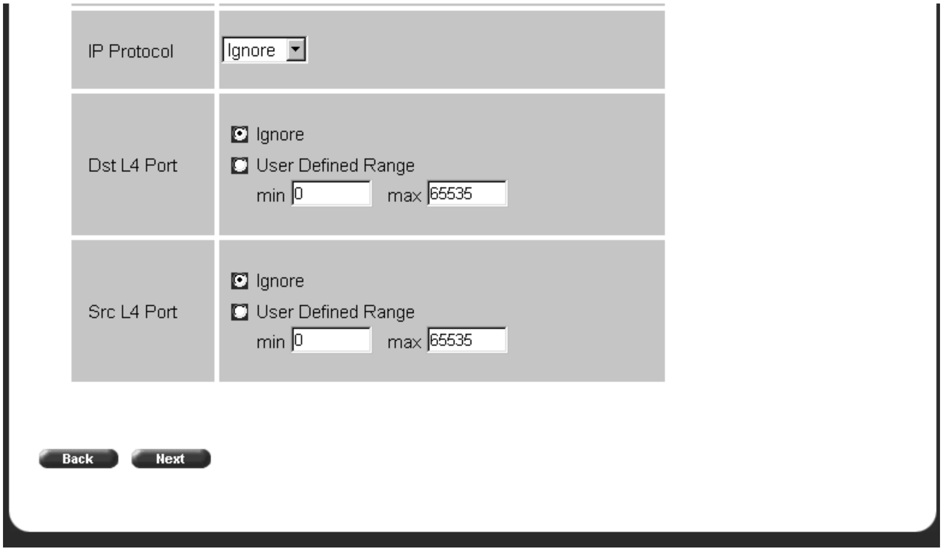
QoS Wizard

Step 1 - Policy Label | **Step 2 - Policy Definition** | Step 3 - Meter | Step 4 - Service | Step 5 - Shap

Select the classification rules for **peggy**:

VLAN	● Ignore ○ VLAN(s) VLAN #1 (maximum 32)
VLAN Tag	Ignore
EtherType	● Ignore ○ Preconfigured Netmap TCP ○ User Defined (e.g. 0x8137)
802.1p Priority	● Ignore ○ Priority ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7
DSCP	Ignore

Figure 121 Layer 2 classification rules page (2 of 2)



IP Protocol: Ignore

Dst L4 Port
● Ignore
○ User Defined Range
min 0 max 65535

Src L4 Port
● Ignore
○ User Defined Range
min 0 max 65535

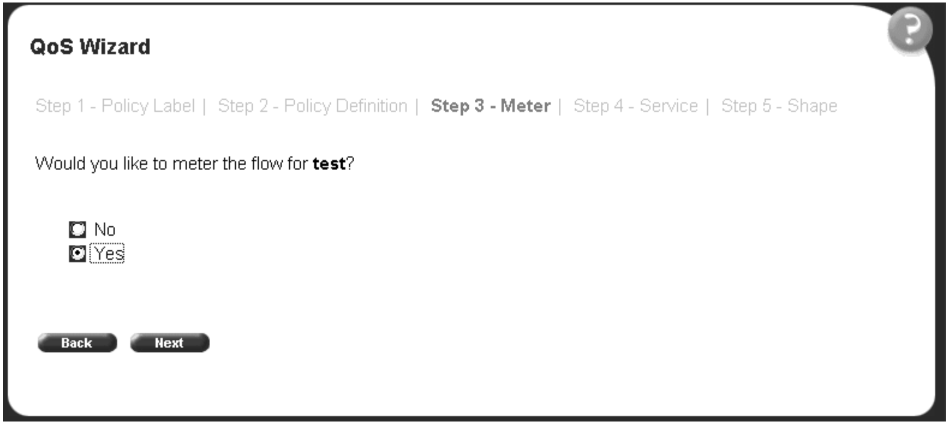
— Choose the layer 2 filter parameters you want the flow to have. (Refer to Chapter 9 for a description of the parameters.)

Beginning with software version 2.0, you can reference up to 32 VLANs with a single layer 2 filter.

— Click Next.

A page opens (Figure 122) that asks if you want to set a Meter for the specified flow.

Figure 122 Meter for user defined flow page



QoS Wizard

Step 1 - Policy Label | Step 2 - Policy Definition | **Step 3 - Meter** | Step 4 - Service | Step 5 - Shape

Would you like to meter the flow for **test**?

○ No
● Yes

Back
Next

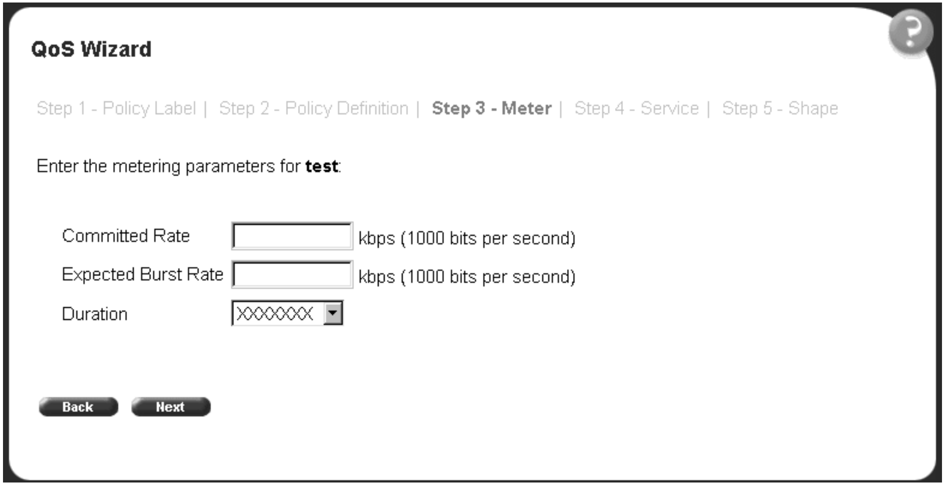
3 If you do not want to set a Meter, click No.

The system opens to the Service Class selection page (Figure 124), which appears with only one Service Class to set. You do not have In-Profile and Out-of-Profile without metering data.

4 If you want to set a Meter, click Yes.

A page opens (Figure 123) that allows you to set a Meter for the specified flow.

Figure 123 Meter setting for user defined flow page



QoS Wizard

Step 1 - Policy Label | Step 2 - Policy Definition | **Step 3 - Meter** | Step 4 - Service | Step 5 - Shape

Enter the metering parameters for **test**:

Committed Rate [ ] kbps (1000 bits per second)
Expected Burst Rate [ ] kbps (1000 bits per second)
Duration XXXXXXX

Back
Next

5 Enter the committed rate you want for this Meter.

6 Enter the expected burst rate you want for this Meter.

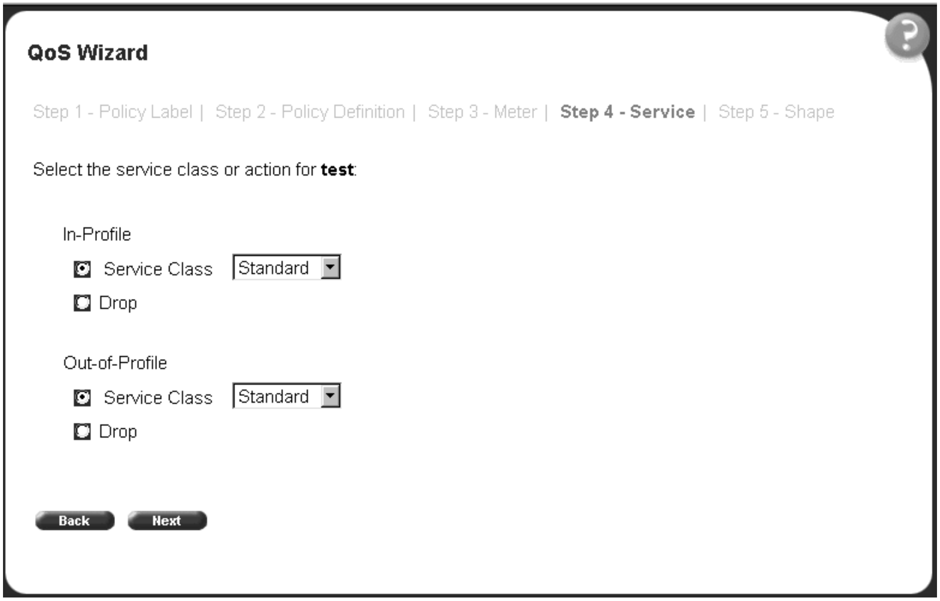
The system calculates a series of 7 or fewer possible durations for the committed and expected burst rates you set.

7 Choose the Duration you want.

8 Click Next.

A page opens (Figure 124) that allows you to select a Service Class separately for both the In-Profile and Out-of-Profile Action for the specified flow.

Figure 124 Service Class selection for user defined flow page



QoS Wizard

Step 1 - Policy Label | Step 2 - Policy Definition | Step 3 - Meter | **Step 4 - Service** | Step 5 - Shape

Select the service class or action for **test**:

In-Profile

● Service Class Standard

○ Drop

Out-of-Profile

● Service Class Standard

○ Drop

9 Click either Service Class or Drop.

If you click Service Class, choose the Service Class you want from the pull-down menu.

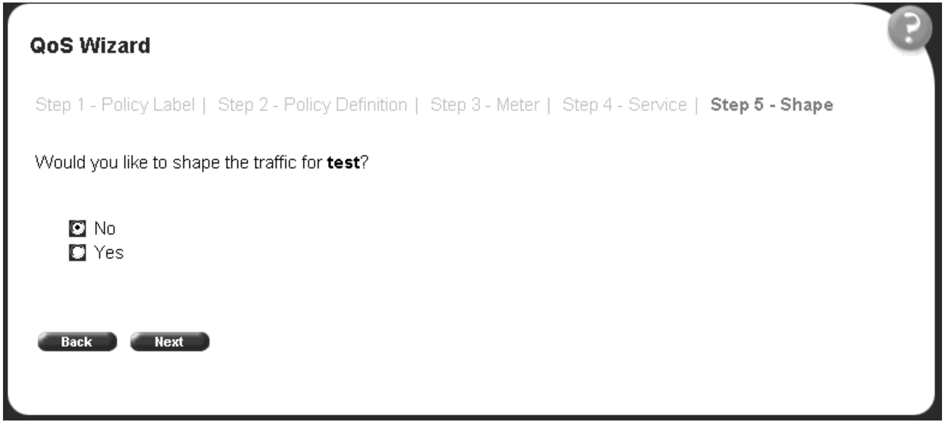
If you click Drop, the traffic in the specified flow is dropped.

10 Click Next.

A page opens (Figure 125) that allows you to set shaping criteria for the specified flow.

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

Figure 125 Shaper for user defined flow page



QoS Wizard

Step 1 - Policy Label | Step 2 - Policy Definition | Step 3 - Meter | Step 4 - Service | **Step 5 - Shape**

Would you like to shape the traffic for **test**?

● No
○ Yes

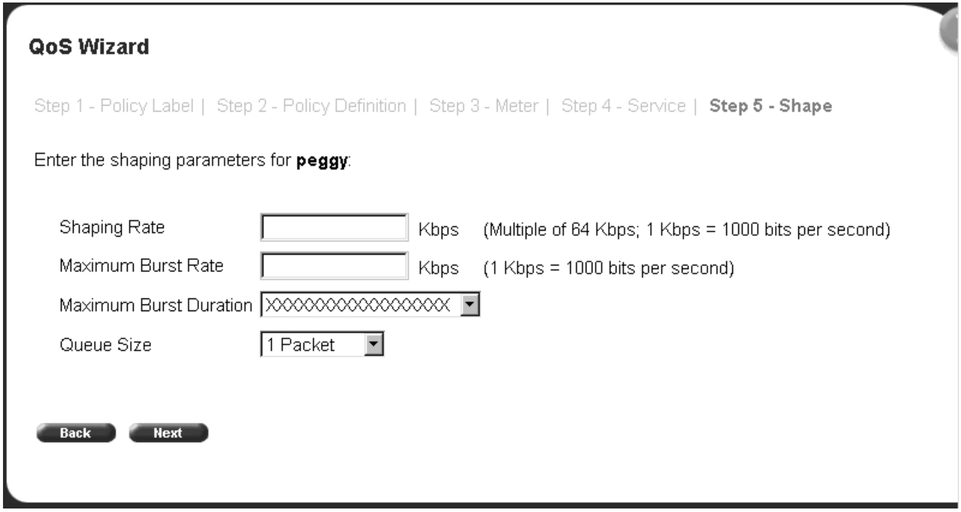
11 If you do not want to shape traffic for the specified flow, click No.

A page opens (Figure 127) that asks if you want to prioritize traffic for another user defined flow.

12 If you want to shape traffic for the specified flow, click Yes.

A page opens (Figure 126) that allows you to set shaping parameters for the specified flow.

Figure 126 Setting shaping parameters for user defined flow page


QoS Wizard
Step 1 - Policy Label | Step 2 - Policy Definition | Step 3 - Meter | Step 4 - Service | Step 5 - Shape
Back
Next

Enter the shaping parameters for **peggy**:

Shaping Rate ____ Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)

Maximum Burst Rate ____ Kbps (1 Kbps = 1000 bits per second)

Maximum Burst Duration XXXXXXXXXXXXXXXXX

Queue Size 1 Packet

13 Enter the shaping rate you want for this Shaper.

The system rounds up shaping rates you enter, including 0, to multiples of 64 Kbps.

14 Enter the maximum burst rate you want for this Shaper.

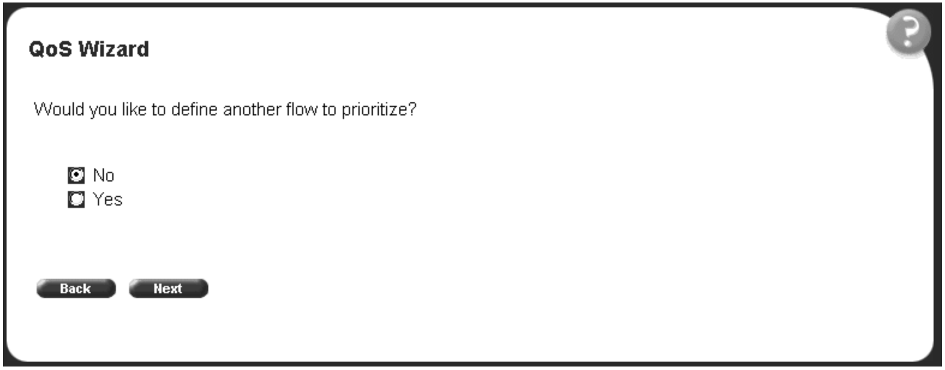
The system calculates a series of 6 or fewer possible durations for the shaping and maximum burst rates you set.

15 Choose the Maximum Burst Duration from the pull-down menu.

16 Choose the queue size you want for this Shaper.

A page opens (Figure 127) that asks you if you want to prioritize traffic for another user defined flow.

Figure 127 Additional user defined flows page



QoS Wizard

Would you like to define another flow to prioritize?

● No
○ Yes

17 If you want to prioritize traffic for another user defined flow, click Yes and Next.

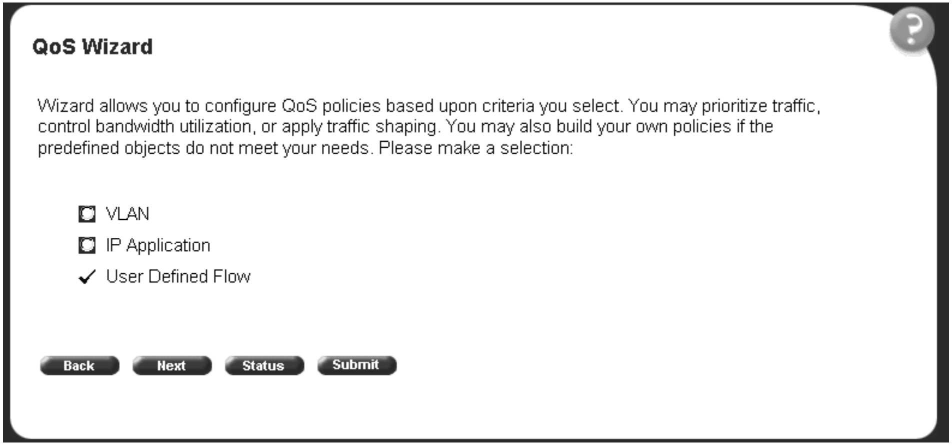
The system returns you to the policy label page (Figure 116), and you continue through steps 1 to 17 for the next user defined flow.

If you fill the resources of the QoS Wizard, you will not be prompted for another user defined flow.

18 If you do not want to prioritize traffic for another user defined flow, click No and Next.

The system returns you to the packet prioritization page (Figure 128), with a check mark next to User Defined Flow. Press the Status button to view the QoS Policies to Configure table listing your new entry in a pop-up window (Figure 129).

Figure 128 Packet prioritization page with prioritized User Defined Flow(s)

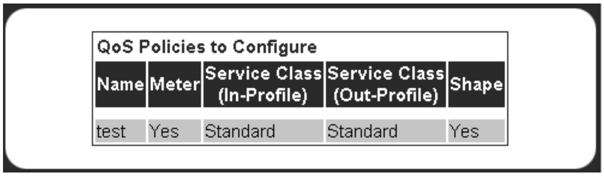


QoS Wizard

Wizard allows you to configure QoS policies based upon criteria you select. You may prioritize traffic, control bandwidth utilization, or apply traffic shaping. You may also build your own policies if the predefined objects do not meet your needs. Please make a selection:

☐ VLAN
☐ IP Application
✓ User Defined Flow

Figure 129 QoS Policies to Configure window with user defined flow entry



QoS Policies to Configure

Name	Meter	Service Class (In-Profile)	Service Class (Out-Profile)	Shape
test	Yes	Standard	Standard	Yes

19 When you are through viewing the table, click Back and then Submit.

You see a session confirmation page.

Using QoS Quick Config

This section describes how to use the QoS Quick Config option to configure QoS parameters for the BPS 2000. This section includes the following topics:

- "Using QoS Quick Config to configure interface groups" on page 237
- "Using QoS Quick Config to configure policies" on page 239

The QoS Quick Config option provides a set of Web pages for configuring QoS parameters. Using the QoS Quick Config does not reset the QoS parameters to default values as the QoS Wizard does. The QoS Quick Config condenses the QoS Advanced pages to just two pages and uses only default actions and mappings.

Using QoS Quick Config to configure interface groups

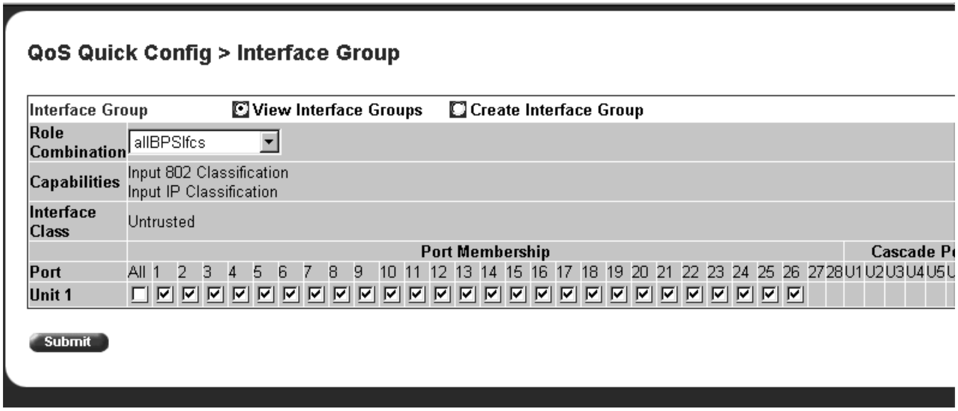
Note: If you do not need to define a new interface group (role combination), you can go directly to "Using QoS Quick Config to configure policies" on page 239.

To use the QoS Quick Config option:

1 From the main menu, choose Application > QoS > QoS Quick Config > Interface Group.

The QoS Quick Config Interface Group page opens (Figure 130) with the View Interface Groups option displaying.

Figure 130 QoS Quick Config Interface Group page—View Interface Group



QoS Quick Config > Interface Group

Interface Group ● View Interface Groups ○ Create Interface Group

Role Combination allBPSIfcs

Capabilities Input 802 Classification
Input IP Classification

Interface Class Untrusted

	Port Membership																												Cascade P					
Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	U1	U2	U3	U4	U5	U
Unit 1	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑								

2 To view the parameters of a specified Interface group, choose the Role Combination (Interface Group) you want to view and use the QoS Quick Config Interface Group page to view the following parameters:

— Capabilities

- Interface Class

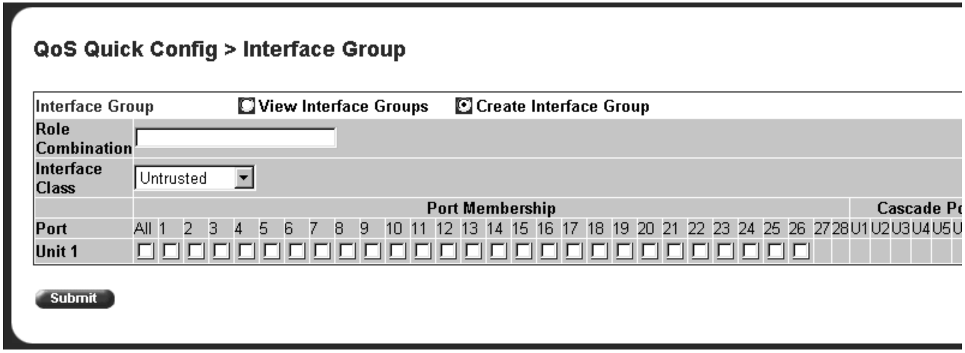
  Refer to *Using the Business Policy Switch 2000 Software Version 2.0* for more information on interface classes.

- Port Membership

3 To create an Interface Group, click Create Interface Group.

The QoS Quick Config Interface Group page opens (Figure 131) with the Create Interface Groups option displaying.

Figure 131 QoS Quick Config Interface Group page—Create Interface Group



QoS Quick Config > Interface Group
Interface Group ○ View Interface Groups ● Create Interface Group
Role Combination
Port Membership
Cascade P
Port All 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 U1 U2 U3 U4 U5 U
Unit 1
Submit

Interface Class: Untrusted

4 Enter the name you want for the new Role Combination (Interface Group).

5 Choose the Interface Class you want from Trusted, Untrusted, or Unrestricted.

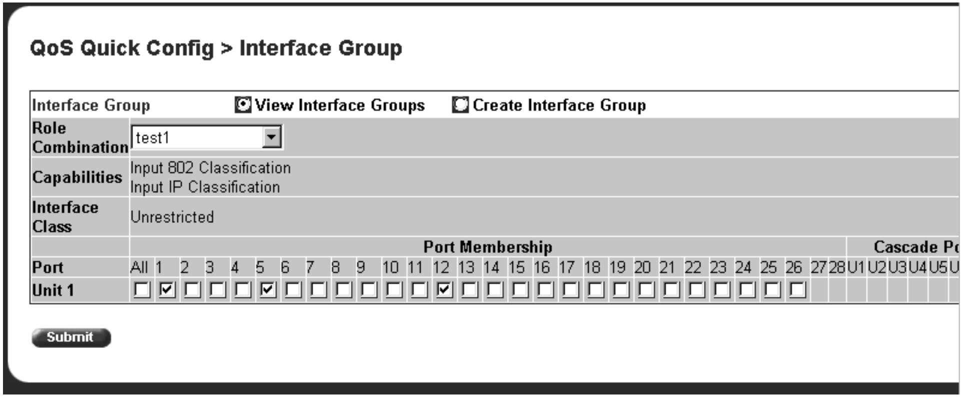
Refer to *Using the Business Policy Switch 2000 Software Version 2.0* for more information on interface classes.

6 Click the ports you want to belong to this Role Combination (Interface Group).

7 Click Submit.

The QoS Quick Config Interface Group page opens (Figure 130) with the View Interface Groups option displaying the new Role combination you just created.

Figure 132 QoS Quick Config Interface Group page—View Interface Group



QoS Quick Config > Interface Group

Interface Group ● View Interface Groups ○ Create Interface Group

Role Combination test1

Capabilities Input 802 Classification
Input IP Classification

Interface Class Unrestricted

	Port Membership																												Cascade P					
Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	U1	U2	U3	U4	U5	U
Unit 1	☐	☑	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐								

8 Go to “Using QoS Quick Config to configure policies,” next.

Using QoS Quick Config to configure policies

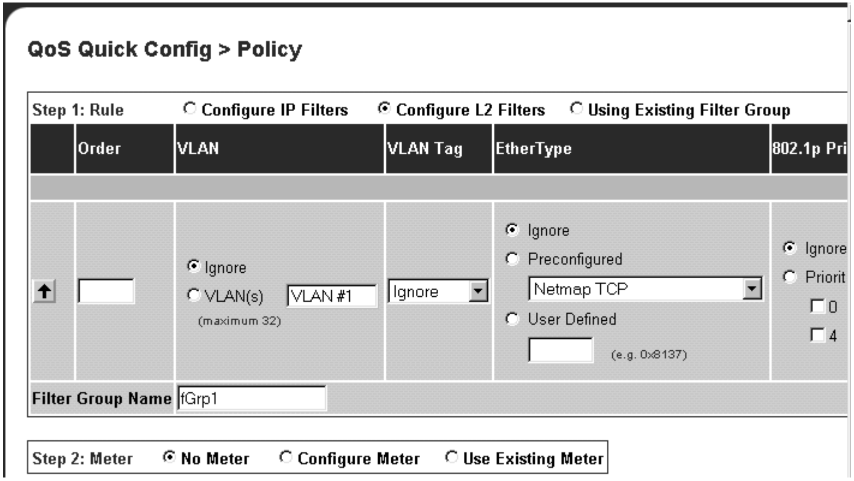
You use QoS Quick Config Web pages to configure the policies.

To configure QoS policies using QoS Quick Config:

➨ From the main menu, choose Application > QoS > QoS Quick Config > Policy.

The QoS Quick Config Policy page opens (Figure 133, Figure 134, and Figure 135).

Figure 133 QoS Quick Config Policy page (1 of 3)



QoS Quick Config > Policy

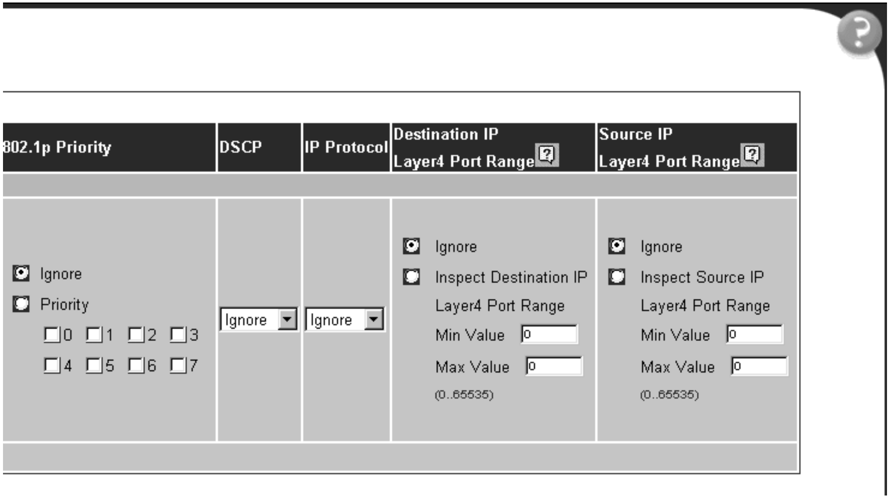
Step 1: Rule ○ Configure IP Filters ● Configure L2 Filters ○ Using Existing Filter Group

	Order	VLAN	VLAN Tag	EtherType	802.1p Pri
↑		● Ignore ○ VLAN(s) VLAN #1 (maximum 32)	Ignore	● Ignore ○ Preconfigured Netmap TCP ○ User Defined (e.g. 0x8137)	● Ignore ○ Priorit ☐ 0 ☐ 4

Filter Group Name fGrp1

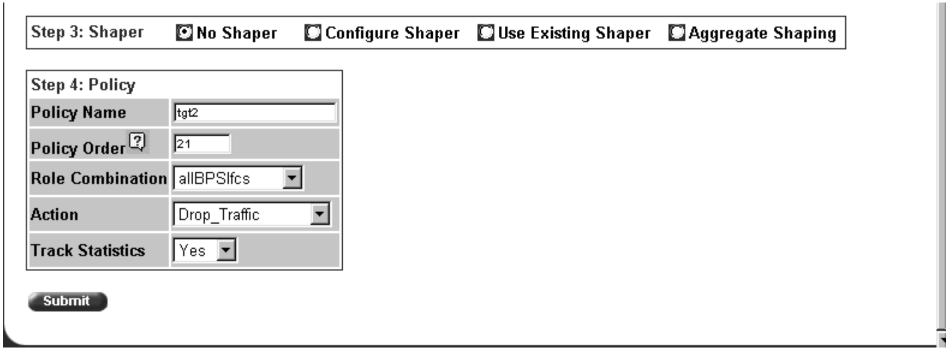
Step 2: Meter ● No Meter ○ Configure Meter ○ Use Existing Meter

Figure 134 QoS Quick Config Policy page (2 of 3)



802.1p Priority	DSCP	IP Protocol	Destination IP Layer4 Port Range	Source IP Layer4 Port Range
● Ignore ○ Priority ☐ 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7	Ignore	Ignore	● Ignore ○ Inspect Destination IP Layer4 Port Range Min Value 0 Max Value 0 (0..65535)	● Ignore ○ Inspect Source IP Layer4 Port Range Min Value 0 Max Value 0 (0..65535)

Figure 135 QoS Quick Config Policy page (3 of 3)



Step 3: Shaper ● No Shaper ○ Configure Shaper ○ Use Existing Shaper ○ Aggregate Shaping

Step 4: Policy

Policy Name	tgt2
Policy Order	21
Role Combination	allBPSIfcs
Action	Drop_Traffic
Track Statistics	Yes

The QoS Quick Config Policy page contains the following four steps:

- Step 1: Rule
- Step 2: Meter
- Step 3: Shaper
- Step 4: Policy

This section discusses the following areas:

- "Configuring QoS Quick Config filters," next
- "Deleting Qos Quick Config filters from the filter group" on page 246
- "Configuring QoS Quick Config meters" on page 247
- "Configuring QoS Quick Config shapers" on page 248
- "Configuring QoS Quick Config policies" on page 250

Configuring QoS Quick Config filters

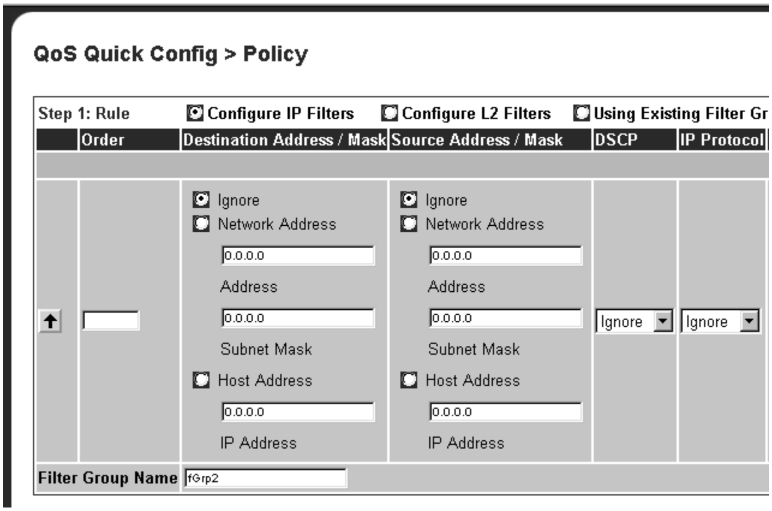
Using Step 1: Rule, you either configure a new filter group or use an existing group.

To configure a new IP filter group:

1 Click Configure IP Filters.

The QoS Quick Config Policy page for configuring IP filters opens (Figure 136 and Figure 137).

Figure 136 QoS Quick Config page for configuring IP filters page (1 of 2)



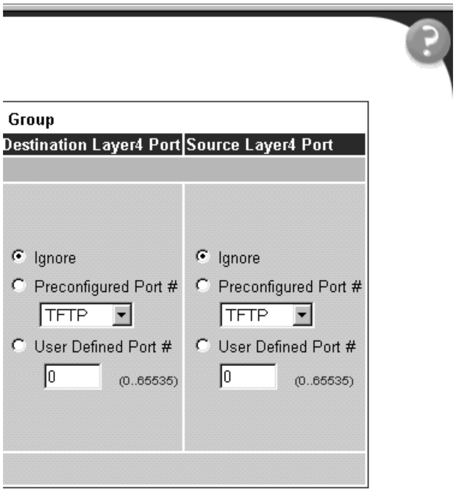
QoS Quick Config > Policy

Step 1: Rule ● Configure IP Filters ○ Configure L2 Filters ○ Using Existing Filter Gr

	Order	Destination Address / Mask	Source Address / Mask	DSCP	IP Protocol
↑		● Ignore ○ Network Address 0.0.0.0 Address 0.0.0.0 Subnet Mask ○ Host Address 0.0.0.0 IP Address	● Ignore ○ Network Address 0.0.0.0 Address 0.0.0.0 Subnet Mask ○ Host Address 0.0.0.0 IP Address	Ignore	Ignore

Filter Group Name: fGrp2

Figure 137 QoS Quick Config page for configuring IP filters page (2 of 2)



Group

Destination Layer4 Port	Source Layer4 Port
● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0 (0..65535)

2 Enter the number you want for the order of the IP filter you are configuring.

3 Complete the Destination Address/Mask area by either:

- — choosing Ignore
- — entering the Network Address, Subnet Mask, and Host Address

4 Complete the Source Address/Mask area by either:

- — choosing Ignore
- — entering the Network Address, Subnet Mask, and Host Address

5 In the DSCP field, choose either Ignore or a value from the pull-down menu.

6 In the IP Protocol field, choose either Ignore or a protocol from the pull-down menu.

7 Complete the Destination Layer4 Port area by either:

- — choosing Ignore
- — choosing a preconfigured port number from the pull-down menu
- — entering a value for the User Defined Port Number

8 Complete the Source Layer4 Port area by either:

- — choosing Ignore
- — choosing a preconfigured port number from the pull-down menu
- — entering a value for the User Defined Port Number

9 Enter the name you want to assign to the newly created IP filter group.

10 Click the arrow on the far left to add the newly created filter into the filter group.

11 Repeat steps 2 to 8 to add additional filters into the filter group.

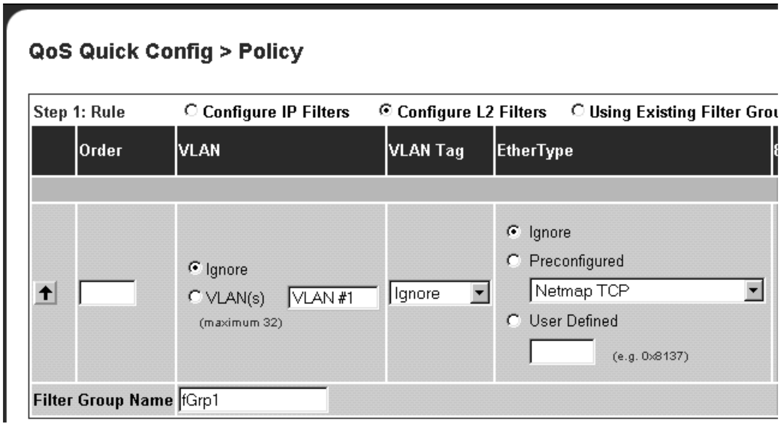
12 Go to "Configuring QoS Quick Config meters" on page 247.

To configure a new layer 2 filter group:

1 Click Configure L2 Filters.

The QoS Quick Config Policy page for configuring layer 2 filters opens (Figure 138 and Figure 139).

Figure 138 QoS Quick Config page for configuring layer 2 filters page (1 of 2)



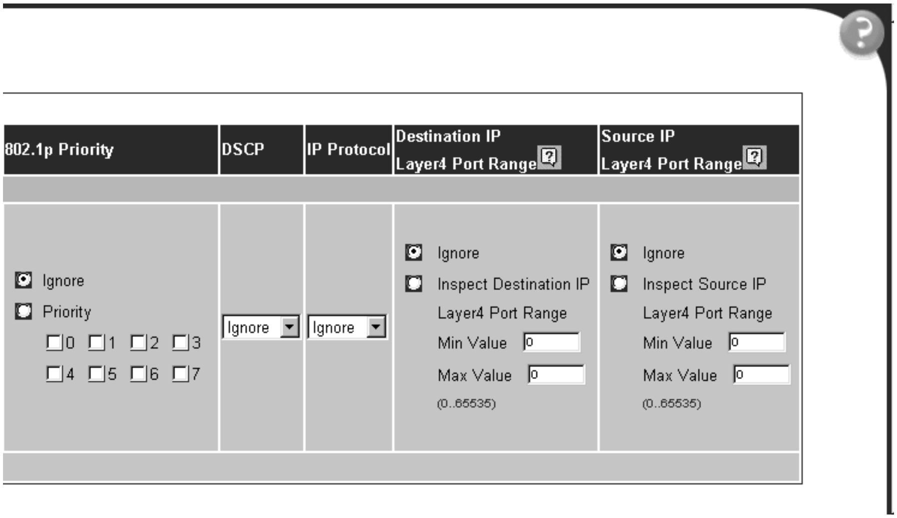
QoS Quick Config > Policy

Step 1: Rule ○ Configure IP Filters ● Configure L2 Filters ○ Using Existing Filter Grou

	Order	VLAN	VLAN Tag	EtherType
		● Ignore ○ VLAN(s) VLAN #1 (maximum 32)	Ignore	● Ignore ○ Preconfigured Netmap TCP ○ User Defined (e.g. 0x8137)

Filter Group Name fGrp1

Figure 139 QoS Quick Config page for configuring layer 2 filters page (2 of 2)



802.1p Priority	DSCP	IP Protocol	Destination IP Layer4 Port Range	Source IP Layer4 Port Range
● Ignore ○ Priority ☐0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7	Ignore	Ignore	● Ignore ○ Inspect Destination IP Layer4 Port Range Min Value 0 Max Value 0 (0..65535)	● Ignore ○ Inspect Source IP Layer4 Port Range Min Value 0 Max Value 0 (0..65535)

2 Enter the number you want for the order of the layer 2 filter you are configuring.

3 In the VLAN area, choose the VLANs you want from the pull-down menu.

Note: Beginning with software version 2.0, you can reference up to 32 VLANs with a layer 2 filter.

4 In the VLAN Tag area, choose either Ignore, Tagged, or Untagged from the pull-down menu.

5 Complete the EtherType area by either:

- choosing Ignore
- choosing a preconfigured Ethernet type from the pull-down menu
- entering a hex value for the User Defined Ethernet type

6 Complete the 802.1p Priority area by either:

- choosing Ignore
- clicking Priority and choosing one of the 0-7 boxes for the priority value

7 In the DSCP field, choose either Ignore or a value from the pull-down menu.

8 In the IP Protocol field, choose either Ignore or a protocol from the pull-down menu.

9 Complete the Destination IP Layer4 Port Range area by either:

- choosing Ignore
- clicking Inspect Destination Layer4 Range and entering a value for both the maximum value and the minimum value

10 Complete the Source IP Layer4 Port Range area by either:

- choosing Ignore
- clicking Inspect Source Layer4 Range and entering a value for both the maximum value and the minimum value

11 Enter the name you want to assign to the newly created layer 2 filter group.

12 Click the arrow on the far left to add the newly created filter into the filter group.

13 Repeat steps 2 to 10 to add additional filters into the filter group.

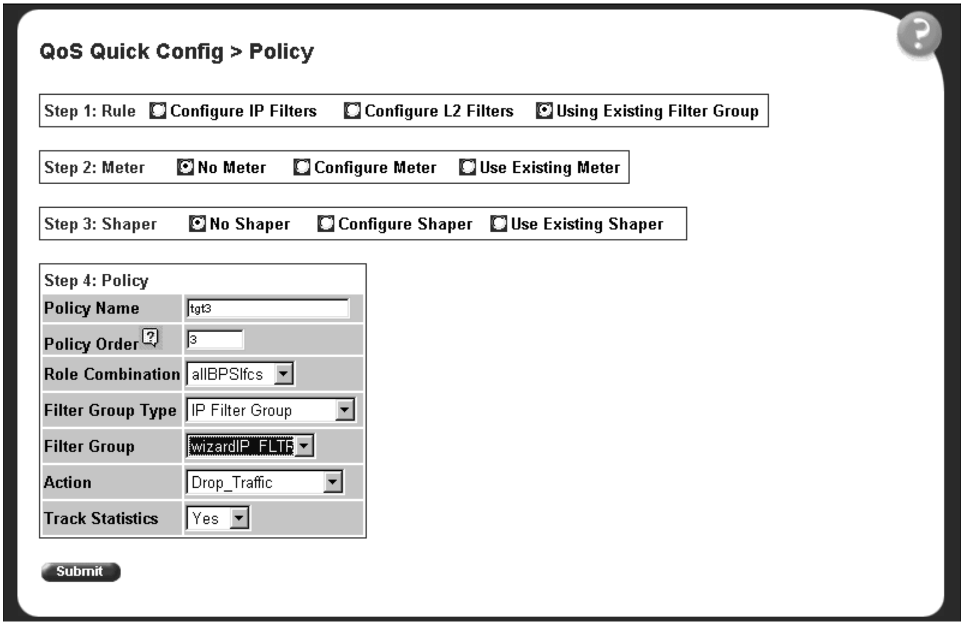
14 Go to“Configuring QoS Quick Config meters” on page 247.

To use an existing filter group:

1 Click Using Existing Filter Group.

A page opens that displays the Using Existing Filter Group option checked (Figure 140).

Figure 140 QoS Quick Config page with existing filter group choice



QoS Quick Config > Policy

Step 1: Rule ○ Configure IP Filters ○ Configure L2 Filters ● Using Existing Filter Group

Step 2: Meter ● No Meter ○ Configure Meter ○ Use Existing Meter

Step 3: Shaper ● No Shaper ○ Configure Shaper ○ Use Existing Shaper

Step 4: Policy	
Policy Name	tgt3
Policy Order	3
Role Combination	allBPSIfcs
Filter Group Type	IP Filter Group
Filter Group	wizardIP_FLTR
Action	Drop_Traffic
Track Statistics	Yes

2 Go to "Configuring QoS Quick Config meters" on page 247.

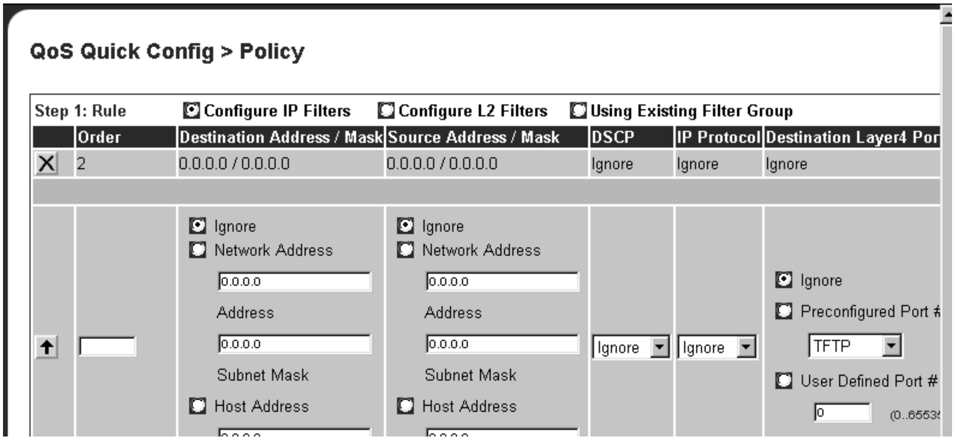
Deleting Qos Quick Config filters from the filter group

The filters of the filter group you created are displayed in a table at the top of the Step 1: Rule section of the QoS Quick Config Policy page. To delete a filter from the filter group:

1 Click QoS Quick Config > Policy.

The filter group you just configured displays in the table at the top of the Step 1: Rule section of the QoS Quick Config Policy page (Figure 141).

Figure 141 QoS Quick Config Policy page with displayed filter group



QoS Quick Config > Policy

Step 1: Rule ● Configure IP Filters ○ Configure L2 Filters ○ Using Existing Filter Group

	Order	Destination Address / Mask	Source Address / Mask	DSCP	IP Protocol	Destination Layer4 Por
X	2	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Ignore	Ignore	Ignore
↑		● Ignore ○ Network Address 0.0.0.0 Address 0.0.0.0 Subnet Mask ○ Host Address	● Ignore ○ Network Address 0.0.0.0 Address 0.0.0.0 Subnet Mask ○ Host Address	Ignore ▾	Ignore ▾	● Ignore ○ Preconfigured Port # TFTP ▾ ○ User Defined Port # 0 (0..6553

2 To delete the filter from the filter group, click the X icon at the far left of the table.

Configuring QoS Quick Config meters

Using Step 2: Meters, you choose to use nonmetered data for specified flow, to configure a new meter for the flow, or to use an existing meter for the flow.

To choose no metered data for the flow:

1 Click No Meter.

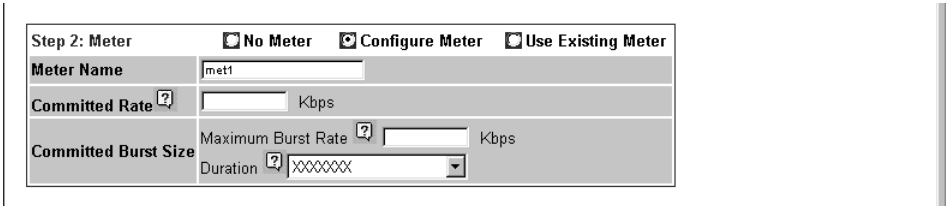
2 Go to “Configuring QoS Quick Config shapers” on page 248.

To create a new meter for the flow:

1 Click Configure Meter.

The system returns a page with the Step 2: Meter area expanded to allow you to configure QoS metering parameters (Figure 142).

Figure 142 QoS Quick Config Policy page with expanded meter area



Step 2: Meter	○ No Meter ● Configure Meter ○ Use Existing Meter
Meter Name	met1
Committed Rate	Kbps
Committed Burst Size	Maximum Burst Rate Kbps Duration XXXXXXX

2 Enter the name you want for the meter in the Meter Name field.

3 In the Committed Rate field, enter the rate you want for your meter.

4 In the Committed Burst Size field

- Enter the burst you want to allow
- Choose among the 6 or fewer durations the system calculates for the meter.

5 Go to "Configuring QoS Quick Config shapers" on page 248.

To use an existing meter for the flow:

1 Click Use Existing Meter.

2 Go to "Configuring QoS Quick Config shapers," next.

Configuring QoS Quick Config shapers

Note: You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

Using Step 3: Shapers, you choose not to shape the data for specified flow, to configure a new shaper for the flow, or to use an existing shaper for the flow, or to reference an aggregate shaping group.

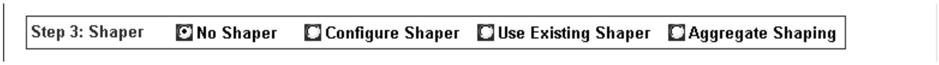
To choose not to shape the data for the flow:

1. Click No Shaper.
2. Go to "Configuring QoS Quick Config policies" on page 250.

To configure a new shaper:

1. Click Configure Shaper, under Step 3: Shaper (Figure 143).

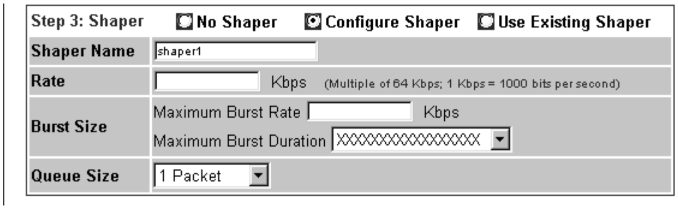
Figure 143 Step 3: Shaper



Step 3: Shaper ● No Shaper ○ Configure Shaper ○ Use Existing Shaper ○ Aggregate Shaping

The Shaper box opens (Figure 144).

Figure 144 Shaper box



Step 3: Shaper ○ No Shaper ● Configure Shaper ○ Use Existing Shaper

Shaper Name	shaper1
Rate	Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)
Burst Size	Maximum Burst Rate Kbps Maximum Burst Duration XXXXXXXXXXXXXXXX
Queue Size	1 Packet

2. Enter the name for the shaper you are configuring in the Shaper Name field.
3. In the Rate field, enter the committed rate you want in Kbps.

   The system rounds up the shaping rate you enter, including 0, to a multiple of 64 Kbps.

4. Enter the maximum rate in Kbps in the Maximum Burst Rate field.
5. Choose the duration from the pull-down menu in the Maximum Burst Duration field.

   The system calculates the durations and presents you with 1 to 6 duration choices.

6 Choose the queue size from the pull-down menu in the Queue Size field.

The queue size is the amount to traffic that can exceed the maximum burst size and still be queued for transmission. This traffic is delayed for shaping purposes.

7 Go to "Configuring QoS Quick Config policies" on page 250.

To use an existing shaper for the flow:

1 Click Use Existing Shaper, under Step 3: Shaper (Figure 143).

2 Go to "Configuring QoS Quick Config policies" on page 250.

To use aggregate shaping for the flow:

1 Click Aggregate Shaping, under Step 3: Shaper (Figure 143).

2 Go to "Configuring QoS Quick Config policies," next.

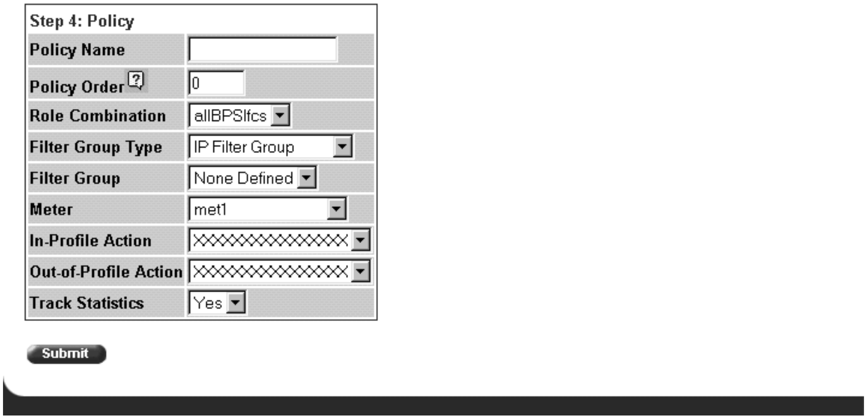
Configuring QoS Quick Config policies

Using the Step 4: Policy area, you apply a policy to the specified flow (Figure 145).

Note: The Step:4 Policy area displays differently, depending on whether you are referencing meters and/or shapers:

- If you are not metering data, only an Action field appears.
- If you are metering data and have already assigned actions to the meter entry, no Action field appears.
- If you are metering data and have not assigned actions to the meter entry, the In-Profile and Out-of-Profile Action fields appear.
- If you are not referencing a shaper or creating a shaper, the Shaper field(s) do not appear.
- If you are referencing an existing shaper, the Shaper Name field appears.
- If you are referencing aggregate shaping, the Shaping Group field appear.

Figure 145 Policy area of QoS Quick Config Policy page

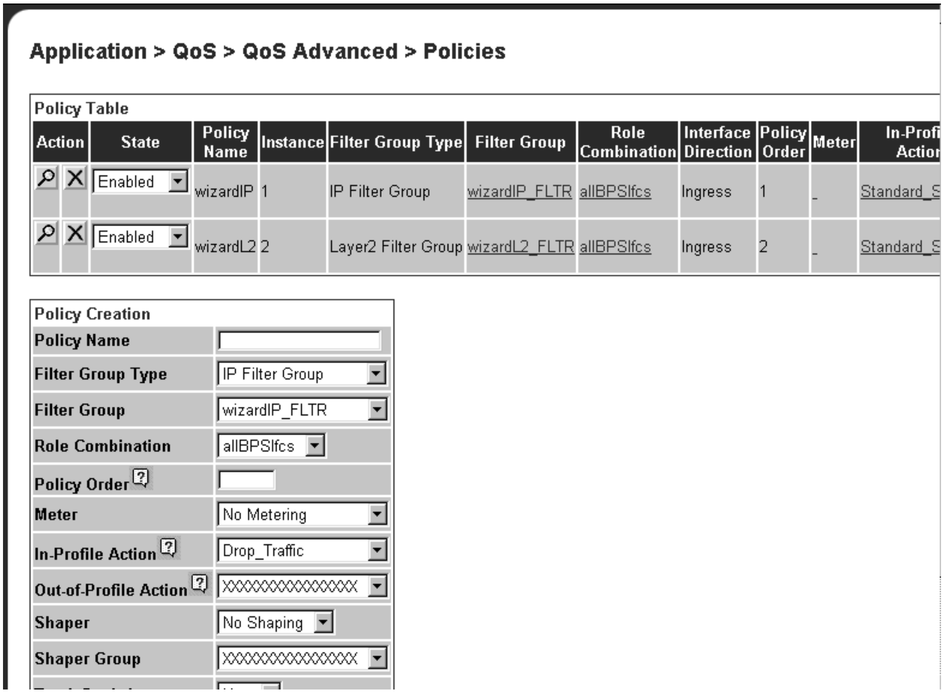


Step 4: Policy	
Policy Name	
Policy Order	0
Role Combination	allBPSIfcs
Filter Group Type	IP Filter Group
Filter Group	None Defined
Meter	met1
In-Profile Action	XXXXXXXXXXXXXXX
Out-of-Profile Action	XXXXXXXXXXXXXXX
Track Statistics	Yes

1. In the Policy Name field, enter a character string to assign a name for the policy you are configuring.
2. In the Policy Order field, enter the value you want for the evaluation order of the policy you are configuring.
3. In the Role Combination field, choose the Role Combination you want.
4. If you are referencing a meter with the policy:
   - Choose the In-Profile Action you want from the pull-down menu.
   - Choose the Out-of-Profile Action you want from the pull-down menu.
5. If you are referencing a existing shaper with the policy, choose the Shaper Name from the pull-down menu.
6. If you are referencing an existing aggregate shaper group with the policy, choose the Shaper Group group from the pull-down menu.
7. In the Track Statistics field, choose Yes or No from the pull-down menu.
8. Click Submit.

   The system returns you to the QoS Advanced Policies page, with your newly configured policy displayed in the Policy Table area (Figure 146 and Figure 147).

Figure 146 QoS Advanced Policies page with configured policies (1 of 2)



Application > QoS > QoS Advanced > Policies

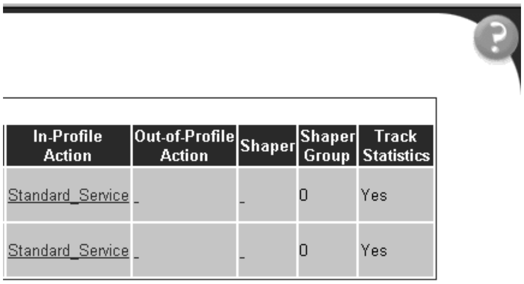
Policy Table

Action	State	Policy Name	Instance	Filter Group Type	Filter Group	Role Combination	Interface Direction	Policy Order	Meter	In-Profi Actio
	Enabled	wizardIP	1	IP Filter Group	wizardIP_FLTR	allBPSIfcs	Ingress	1	_	Standard_S
	Enabled	wizardL2	2	Layer2 Filter Group	wizardL2_FLTR	allBPSIfcs	Ingress	2	_	Standard_S

Policy Creation

Policy Name	
Filter Group Type	IP Filter Group
Filter Group	wizardIP_FLTR
Role Combination	allBPSIfcs
Policy Order	
Meter	No Metering
In-Profile Action	Drop_Traffic
Out-of-Profile Action	XXXXXXXXXXXXXXXX
Shaper	No Shaping
Shaper Group	XXXXXXXXXXXXXXXX

Figure 147 QoS Advanced Policies page with configured policies (2 of 2)



In-Profile Action	Out-of-Profile Action	Shaper	Shaper Group	Track Statistics
Standard_Service	_	_	0	Yes
Standard_Service	_	_	0	Yes

Chapter 9
Implementing QoS using QoS Advanced

The QoS application delivers a set of tools that, when optimally configured, combats escalating bandwidth costs and optimizes application performance in your network.

QoS tools allow you to prioritize your critical applications and sensitive traffic. You can tailor appropriate services to support this traffic over the wide area, thus maintaining the necessary performance levels on an end-to-end basis.

You can configure Quality of Service (QoS) features in your network by using the Web-based QoS Wizard, using the QoS Quick Config pages, or using the Advanced QoS configuration pages available in the Web-based management user interface. (Refer to Chapter 8 for descriptions of the QoS Wizard and QoS Quick Config options.)

Refer to *Using the Business Policy Switch 2000 Software Version 2.0.* for a sample QoS configuration using the advanced QoS Web pages.

This chapter explains configuring QoS using the Advanced QoS pages. The chapter covers the following topics:

- "Configuring an interface group," next
- "Configuring 802.1p priority queue assignment" on page 261
- "Configuring 802.1p priority mapping" on page 263
- "Creating a DSCP queue assignment" on page 264
- "Configuring DSCP mapping" on page 265
- "IP filter and IP filter group configurations" on page 268
- "Layer 2 filter and layer 2 filter group configurations" on page 278
- "Configuring QoS actions" on page 288
- "Configuring QoS meters" on page 291

- "Configuring QoS shapers" on page 294
- "Configuring QoS policies" on page 297
- "Configuring QoS Policy Agent (QPA) characteristics" on page 304

Note: To configure the features introduced with software version 1.2 and higher in a mixed stack, you must access a BPS 2000 unit.

Configuring an interface group

You view existing interface group configurations, or create or modify an interface group if you want a port (or ports) to assign the same QoS policy to all interfaces in the group.

Note: One default role combination covers all ports of the device.

Creating an interface group configuration

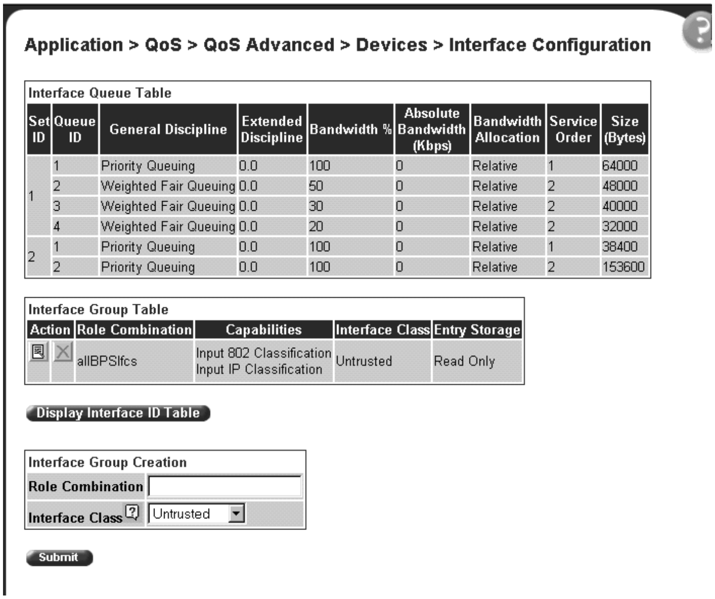
Note: For more information on QoS interface groups, or role combinations, refer to *Using the Business Policy Switch 2000 Software Version 2.0.*

To create an interface group configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

   The Interface Configuration page opens (Figure 148).

Figure 148 QoS Advanced Interface Configuration page



Application > QoS > QoS Advanced > Devices > Interface Configuration

Interface Queue Table

Set ID	Queue ID	General Discipline	Extended Discipline	Bandwidth %	Absolute Bandwidth (Kbps)	Bandwidth Allocation	Service Order	Size (Bytes)
1	1	Priority Queuing	0.0	100	0	Relative	1	64000
	2	Weighted Fair Queuing	0.0	50	0	Relative	2	48000
	3	Weighted Fair Queuing	0.0	30	0	Relative	2	40000
	4	Weighted Fair Queuing	0.0	20	0	Relative	2	32000
2	1	Priority Queuing	0.0	100	0	Relative	1	38400
	2	Priority Queuing	0.0	100	0	Relative	2	153600

Interface Group Table

Action	Role Combination	Capabilities	Interface Class	Entry Storage
▤ ✕	allBPSIfcs	Input 802 Classification Input IP Classification	Untrusted	Read Only

Interface Group Creation

Role Combination	
Interface Class	Untrusted

Table 77 describes the items on the Interface Queue Table section of the QoS Advanced Interface Configuration page.

Table 77 QoS Interface Queue Table section items

Item	Description
Set ID	The number that identifies a specific queue set.
Queue ID	The number that identifies the queue in the given set.
General Discipline	The queueing discipline that is associated with the specified queue. The options are: (1) Other - Use gosIfQueueExtDiscipline, (2) fifo - First In First Out Queuing, (3) pq -Priority Queuing, (4) fg - Fair Queuing, and (5) wfq - Weighted Fair Queuing
Extended Discipline	The queueing discipline that is associated with the specified queue. This attribute provides a means to add additional queueing mechanisms.
Bandwidth	The percentage of available bandwidth consumable to service the queue in one cycle.
Absolute Bandwidth	The absolute bandwidth consumable to service the queue in one cycle.
Bandwidth Allocation	Displays whether absolute or relative bandwidth is specified.
Service Order	The order in which a queue is serviced based on the defined discipline.
Size	The maximum size of the queue in bytes.

Table 78 describes the items on the Interface Group Table section of the QoS Advanced Interface Group page.

Table 78 Interface Group Table section items

Item	**Description**
📝	Opens a modification page.
☒	Deletes the row.
Role Combination	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance (string 1..64). These identifiers are used within a number of classes to logically identify a physical set of interfaces to which policy rules and actions are applied.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select which policies and configurations may be pushed to the Policy Enforcement Point (PEP). The options are: (0) Other, (1) InputIpClassification, (2) output Ip Classification, (3) input 802 Classification, (4) output 802 Classification, (5) single Queuing Discipline, and (6) hybrid Queuing Discipline.
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted, Untrusted, and Unrestricted.
Entry Storage	Specifies whether or not the interface group can be deleted.

Note: For more information on QoS interface classes—or trusted, untrusted, and unrestricted ports—refer to *Using the Business Policy Switch 2000 Software Version 2.0.*

Table 79 describes the items on the Interface Group Creation section of the QoS Advanced Interface Group page.

Table 79 Interface Group Creation section page items

Item and MIB association	Range	Description
Role Combination (qosInterfaceTypeRoles)	1..64	Type a character string to identify the role combination.
Interface Class (qosInterfaceTypeExtIfClass)	(1) Trusted (2) Untrusted (3) Unrestricted	Choose an interface class: Selecting Trusted requests the incoming DSCP value to not be changed, and instead be used for 802.1p user priority and queue assignment based on values in the DSCP mapping table and DSCP mapping table. Selecting Untrusted forces the incoming DSCP value (and associated mappings) to modify to a standard value by default. Actions associated with untrusted interfaces must re-mark the DSCP. Selecting Unrestricted allows you to configure actions that: • re-mark the DSCP or leave the DSCP as is • re-mark the 802.1p priority value or leave as is

2 In the Interface Group Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new interface group configuration appears in the Interface Group Table (Figure 148)

Displaying Interface ID Table

To display the Interface ID Table:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

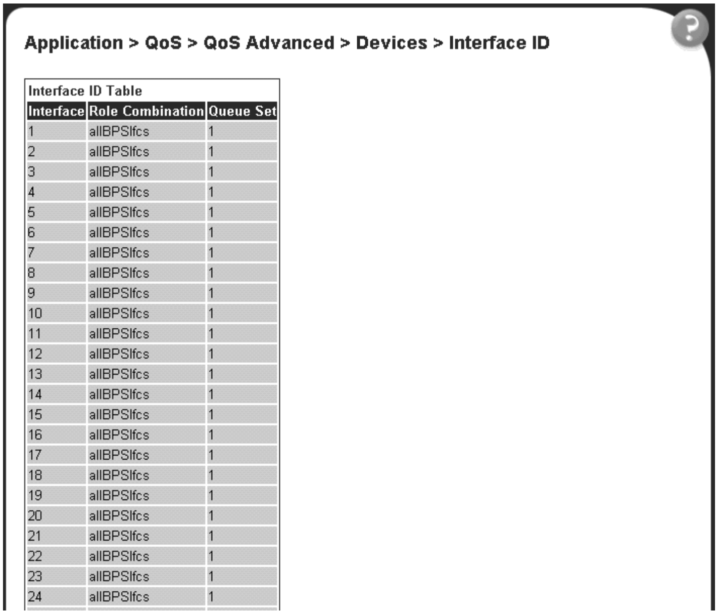
The QoS Advanced Interface Configuration page opens (Figure 148).

2 Click Display Interface ID Table.

The Interface ID page opens (Figure 149). The table displays all interfaces and the interface group (role combination) to which it belongs. If an interface does not belong to an interface group (role combination), it does not display in the table.

The table displays all created interface groups, whether created using the Qos Advanced pages, the QoS Wizard, or the QoS Quick config.

Figure 149 Interface ID page



Interface ID Table

Interface	Role Combination	Queue Set
1	allBPSIfcs	1
2	allBPSIfcs	1
3	allBPSIfcs	1
4	allBPSIfcs	1
5	allBPSIfcs	1
6	allBPSIfcs	1
7	allBPSIfcs	1
8	allBPSIfcs	1
9	allBPSIfcs	1
10	allBPSIfcs	1
11	allBPSIfcs	1
12	allBPSIfcs	1
13	allBPSIfcs	1
14	allBPSIfcs	1
15	allBPSIfcs	1
16	allBPSIfcs	1
17	allBPSIfcs	1
18	allBPSIfcs	1
19	allBPSIfcs	1
20	allBPSIfcs	1
21	allBPSIfcs	1
22	allBPSIfcs	1
23	allBPSIfcs	1
24	allBPSIfcs	1

Table 81 describes the items on the Interface ID page.

Table 80 Interface ID page items

Item	Description
Interface	Displays the unit and port number.
Role Combination	Displays the role combination associated with the interface.
Queue Sets	Displays the queue set associated with this interface.

Adding or removing interface group members

To select or deselect ports as members of an existing interface group:

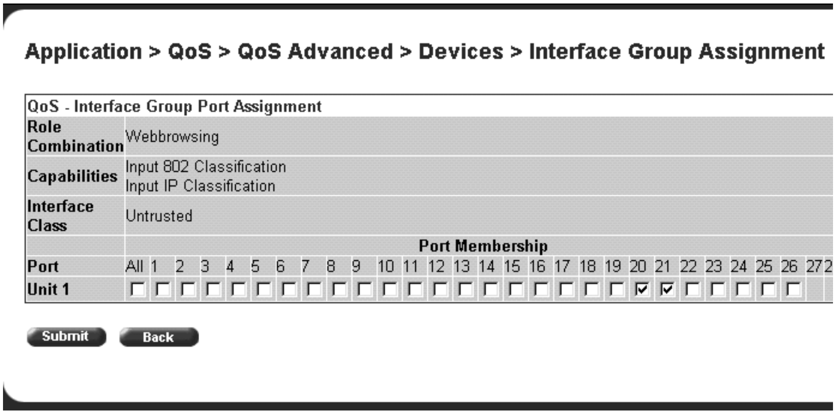
1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

The QoS Advanced Interface Configuration page opens (Figure 148).

2 In the Interface Group Table section, in the row of your choice, click the Modify icon.

The Interface Group Assignment page opens (Figure 150).

Figure 150 Interface Group Assignment page



Application > QoS > QoS Advanced > Devices > Interface Group Assignment

QoS - Interface Group Port Assignment

Role Combination	Webbrowsing
Capabilities	Input 802 Classification Input IP Classification
Interface Class	Untrusted

Port Membership

Port	All	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	2
Unit 1	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☑	☑	☐	☐	☐	☐	☐		

Table 81 describes the items on the Interface Group Assignment page.

Table 81 Interface Group Assignment page items

Item	Description
Role Combination	The tag used to identify interfaces with the characteristics specified by the attributes of this class instance (string 1..64). These identifiers are used within a number of classes to logically identify a physical set of interfaces to which policy rules and actions are applied. This is the group of interfaces (interface group) to which policy rules and actions are applied.
Capabilities	A list of the interface capabilities used by the PDP or network manager to select which policies and configurations may be pushed to the Policy Enforcement Point (PEP). The options are: (0) Other, (1) Input Ip Classification, (2) output Ip Classification, (3) input 802 Classification, (4) output 802 Classification, (5) single Queuing Discipline, and (6) hybrid Queuing Discipline
Interface Class	The type of traffic received on interfaces associated with the specified role combination. The options are Trusted, Untrusted, and Unrestricted.
Port Membership	Select the external ports to associate with the interface group, or select ALL to associate all ports on that unit.
Cascade Ports	The cascade (internal) ports to associate with the interface group.

3 In the Port Membership section, click the check boxes of the ports (or ALL to select all ports on the unit) to associate with the interface group.

Note: Beginning with software version 2.0, you can add all ports of one unit simultaneously, by clicking All. Also, if you are using stacked BPS 2000, you can modify, add, or delete the interfaces of only one unit at a time.

4 Do one of the following:

- Click Submit.
- Click Back to return to the Interface Configuration page without making changes.

Deleting an interface group configuration

To delete an Interface group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Interface Configuration.

The QoS Advanced Interface Configuration page opens (Figure 148).

2 In the Interface Group Table section, in the interface group configuration row of your choice, click the Modify icon.

The Interface Group Assignment page opens (Figure 150).

3 In the Port Membership section, click the check boxes to deselect all ports associated with the interface group.

Note: Beginning with software version 2.0, you can delete all ports of one unit simultaneously, by clicking All.

4 Click Submit.

The Interface Configuration page is displayed (Figure 148).

5 In the Interface Group Table section, in the configuration row of your choice, click the Delete icon.

   A message opens prompting you to confirm your request.

6 Do one of the following:

   - Click Yes to delete the interface group configuration.
   - Click Cancel to return to the Interface Configuration page without making changes.

Configuring 802.1p priority queue assignment

➡ **Note:** Nortel Networks recommends using the default 802.1p assignments to ensure end-to-end QoS connectivity.

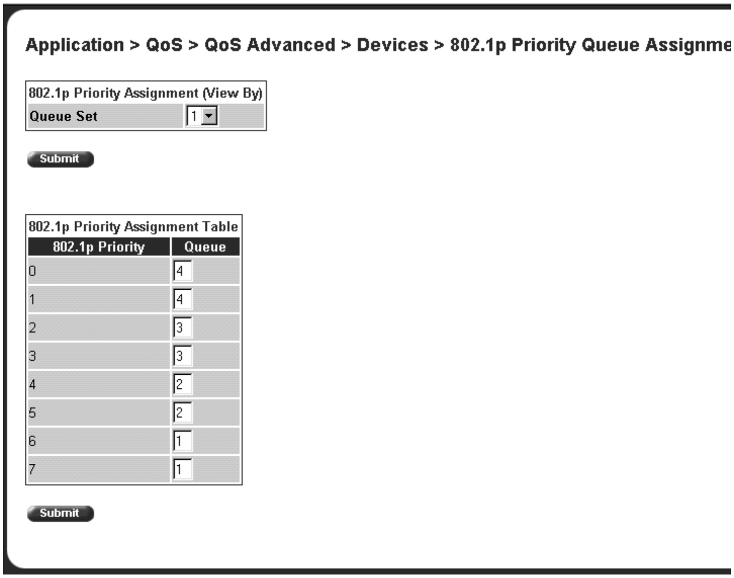
You can assign 802.1p user priority values to a queue for each interface with a specific queue set. This information is used for assigning egress traffic to outbound queues.

To configure 802.1p user priority:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Priority Q Assign.

   The 802.1p Priority Queue Assignment page opens (Figure 151).

Figure 151 802.1p Priority Queue Assignment page



Application > QoS > QoS Advanced > Devices > 802.1p Priority Queue Assignme

802.1p Priority Assignment (View By)

Queue Set: 1

802.1p Priority Assignment Table

802.1p Priority	Queue
0	4
1	4
2	3
3	3
4	2
5	2
6	1
7	1

Table 82 describes the items on the 802.1p Priority Queue Assignment page.

Table 82 802.1p Priority Assignment Table section page items

Section	Item and MIB association	Description
802.1p Priority Assignment (View By)	Queue Set	Choose the queue set you want to modify.
802.1p Priority Assignment Table	802.1p Priority (ntnQosIfPriAssignmentPri)	The 802.1p user priority mapped to a queue.
	Queue (ntnQosIfPriAssignmentQueuet)	Type a number that signifies the desired queue in the specified queue set with which this priority is associated.

2 In the 802.1p Priority Assignment section, select the queue set to view in the 802.1p Priority Assignment Table.

3 Click Submit

The table is updated with the queue set you requested.

4 In the 802.1p Priority Assignment Table section, type the information in the text boxes.

5 Click Submit.

Note: Clicking Submit in the 802.1p Priority Assignment Table section results in a system reset.

Configuring 802.1p priority mapping

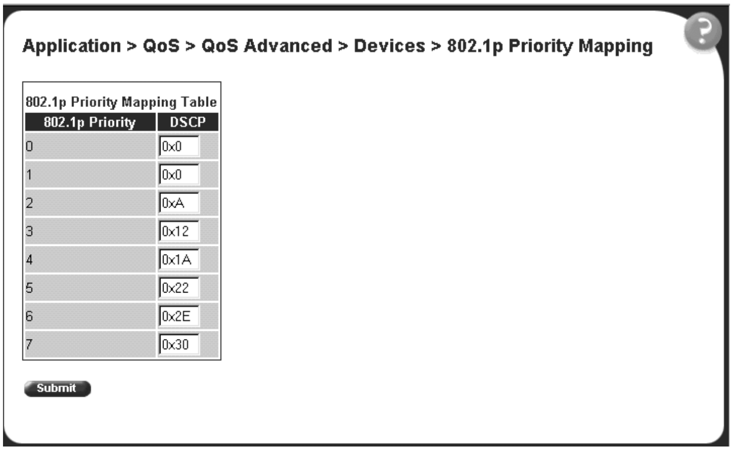
Note: Nortel Networks recommends using the default 802.1p priority to DSCP mappings to ensure end-to-end QoS connectivity.

To configure 802.1p priority to DSCP mapping:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > Priority Mapping.

The 802.1p Priority Mapping page opens (Figure 152).

Figure 152 802.1p Priority Mapping page


Application > QoS > QoS Advanced > Devices > 802.1p Priority Mapping
Submit

802.1p Priority Mapping Table

802.1p Priority	DSCP
0	0x0
1	0x0
2	0xA
3	0x12
4	0x1A
5	0x22
6	0x2E
7	0x30

Table 83 describes the items on the 802.1p Priority Mapping page.

Table 83 802.1p Priority Mapping page items

Item	Description
802.1p Priority	The 802.1p user priority to map to a DSCP value at ingress.
DSCP	Type the DSCP value to associate with the specified 802.1p user priority value at ingress.

2 Type the information in the text boxes.

3 Click Submit.

Creating a DSCP queue assignment

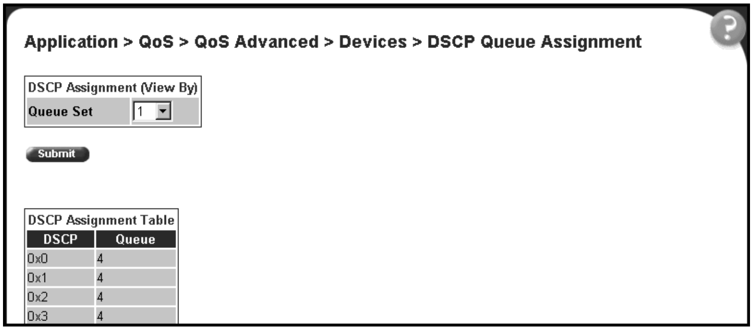
Note: Nortel Networks recommends using the default DSCP to queue set mappings to ensure end-to-end QoS connectivity.

To create a DSCP/queue set association:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > DSCP Q Assignment.

The DSCP Queue Assignment page opens (Figure 153).

Figure 153 DSCP Queue Assignment page


Application > QoS > QoS Advanced > Devices > DSCP Queue Assignment
Submit

DSCP Assignment (View By)

Queue Set: 1

DSCP Assignment Table

DSCP	Queue
0x0	4
0x1	4
0x2	4
0x3	4

Table 84 describes the items on the DSCP Queue Assignment page.

Table 84 DSCP Queue Assignment page items

Section	Item	Format
DSCP Assignment (View By)	Queue Set	Choose the queue set to display in the DSCP Assignment Table.
DSCP Assignment Table	DSCP	The DSCP value to map to a queue.
	Queue	The queue set to which the traffic with the given DSCP value is associated.

2 In the DSCP Assignment (View By) section, choose the queue set to display in the DSCP Assignment Table.

The table is updated with information for the selected queue.

3 In the DSCP Assignment Table section, type the information in the text boxes.

4 Click Submit.

Configuring DSCP mapping

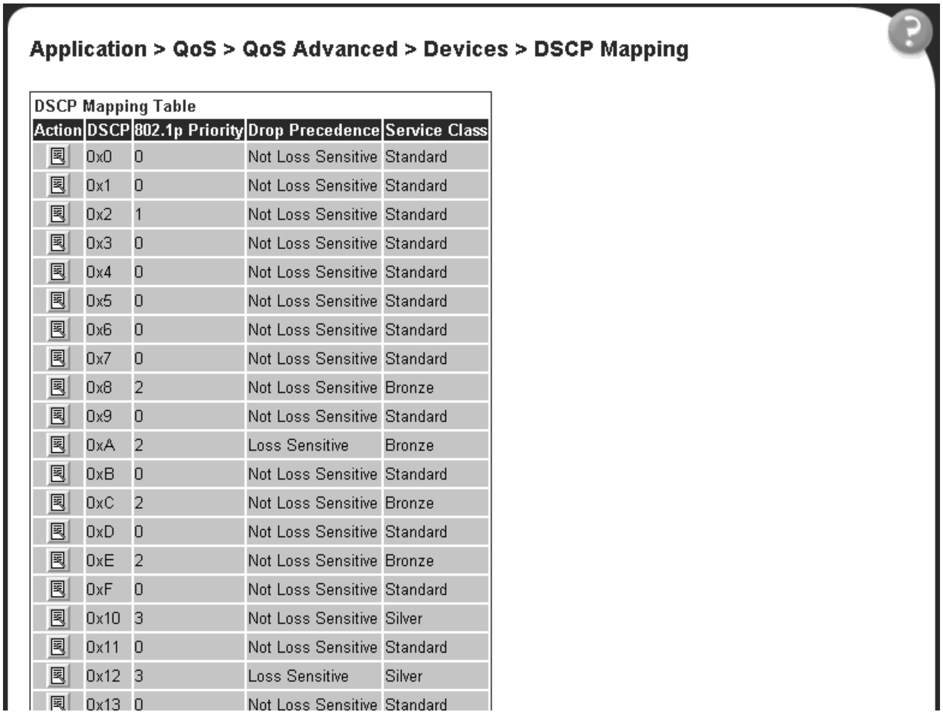
Note: Nortel Networks recommends using the default DSCP mappings to ensure end-to-end QoS connectivity.

To configure DSCP to 802.1p user priority/drop precedence mapping:

1 From the main menu, choose Application > QoS > QoS Advanced > Devices > DSCP Mapping.

The DSCP Mapping page opens (Figure 154).

Figure 154 DSCP Mapping Table page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Table

Action	DSCP	802.1p Priority	Drop Precedence	Service Class
✎	0x0	0	Not Loss Sensitive	Standard
✎	0x1	0	Not Loss Sensitive	Standard
✎	0x2	1	Not Loss Sensitive	Standard
✎	0x3	0	Not Loss Sensitive	Standard
✎	0x4	0	Not Loss Sensitive	Standard
✎	0x5	0	Not Loss Sensitive	Standard
✎	0x6	0	Not Loss Sensitive	Standard
✎	0x7	0	Not Loss Sensitive	Standard
✎	0x8	2	Not Loss Sensitive	Bronze
✎	0x9	0	Not Loss Sensitive	Standard
✎	0xA	2	Loss Sensitive	Bronze
✎	0xB	0	Not Loss Sensitive	Standard
✎	0xC	2	Not Loss Sensitive	Bronze
✎	0xD	0	Not Loss Sensitive	Standard
✎	0xE	2	Not Loss Sensitive	Bronze
✎	0xF	0	Not Loss Sensitive	Standard
✎	0x10	3	Not Loss Sensitive	Silver
✎	0x11	0	Not Loss Sensitive	Standard
✎	0x12	3	Loss Sensitive	Silver
✎	0x13	0	Not Loss Sensitive	Standard

Table 85 describes the items on the DSCP Mapping Table page.

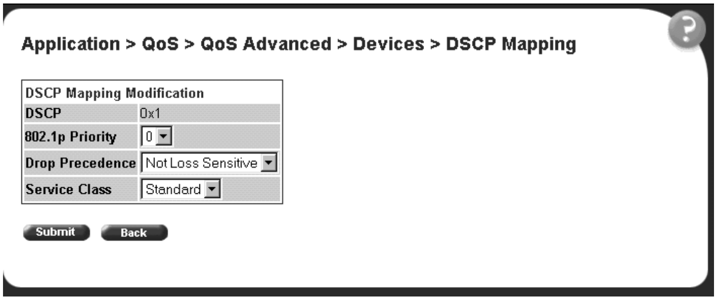
Table 85 DSCP Mapping Table page items

Item	Format
✎	Opens a modification page.
DSCP	The attribute used internally to determine the appropriate Layer 2 cost of service (CoS) mappings.
802.1p Priority	The IEEE802 CoS value used when mapping the DSCP value specified by the qos802DscpMappingDscp attribute to an IEEE 802 CoS.
Drop Precedence	The drop value precedence used for traffic with the associated 802.1D user priority value with the identified queue. Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	The current service class. The options are: Standard, Bronze, Silver, Gold, Platinum, Premium, and Network. Note: This field corresponds to the adjacent user priority levels.

2 In the row of your choice, click the Modification icon.

The DSCP Mapping Modification page opens (Figure 155).

Figure 155 DSCP Mapping Modification page



Application > QoS > QoS Advanced > Devices > DSCP Mapping

DSCP Mapping Modification	
DSCP	0x1
802.1p Priority	0
Drop Precedence	Not Loss Sensitive
Service Class	Standard

Table 86 describes the items on the DSCP Mapping Modification page.

Table 86 DSCP Mapping Modification page items

Item	Range	Format
DSCP	0..63	Type the attribute to use internally to determine the appropriate Layer 2 cost of service (CoS) mappings.
802.1p Priority	0..7	Choose the IEEE802 CoS value to use when mapping the DSCP value specified by the qos802DscpMappingDscp attribute to an IEEE 802 CoS.
Drop Precedence	Loss Sensitive Not Loss Sensitive	Choose the drop value precedence to use for traffic with the associated 802.1p user priority value with the identified queue. Selecting a Loss Sensitive value specifies a low packet drop precedence; selecting a Not Loss Sensitive value specifies a high packet drop precedence. Note: Generally, low packet drop precedence receives preferential treatment.
Service Class	Standard Bronze Silver Gold Platinum Premium Network	Choose the service class. Note: This field corresponds to the adjacent user priority levels.
	Note: Mappings created on the DSCP mapping modification page are used at egress for marking traffic: Trusted and unrestricted IP traffic—If you select the re-marking action of using the egress map, the mappings determine the 802.1p priority and drop precedence values associated with packets based on the DSCP of the received packet. Untrusted and untresticted traffic—If you select the re-marking action of using default, the mappings determine the 802.1p priority and drop precedence values associated with packets based on the DSCP value you specified in the Update DSCP action field.	

3 Select from a list.

4 Click Submit.

The modified configuration appears in the DSCP Mapping Table (Figure 154).

Note: For more information on QoS interface classes—or trusted, untrusted, and unrestricted ports—refer to *Using the Business Policy Switch 2000 Software Version 2.0*.

IP filter and IP filter group configurations

You can create an IP filter, which enables the switch to classify traffic. In turn, you can create an access control list from a series of defined filters to create an IP filter group. The filter group then determines access to and denial of network services.

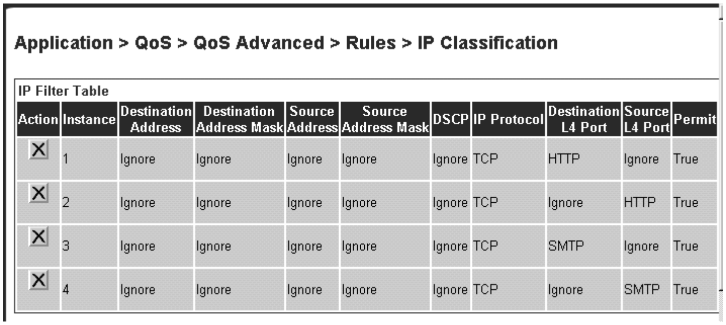
Creating an IP filter configuration

To create an IP filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 156, Figure 157, and Figure 158).

Figure 156 IP Classification page (1 of 3)

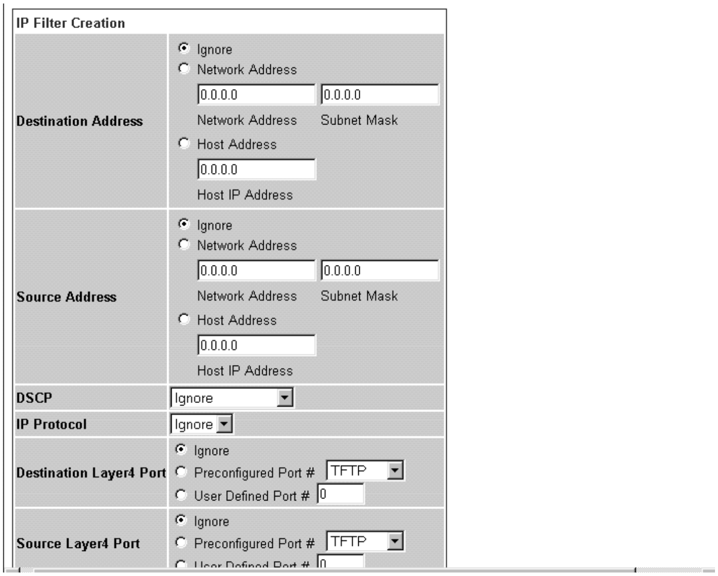


Application > QoS > QoS Advanced > Rules > IP Classification

IP Filter Table

Action	Instance	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	IP Protocol	Destination L4 Port	Source L4 Port	Permit
☒	1	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	HTTP	Ignore	True
☒	2	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	HTTP	True
☒	3	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	SMTP	Ignore	True
☒	4	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	SMTP	True

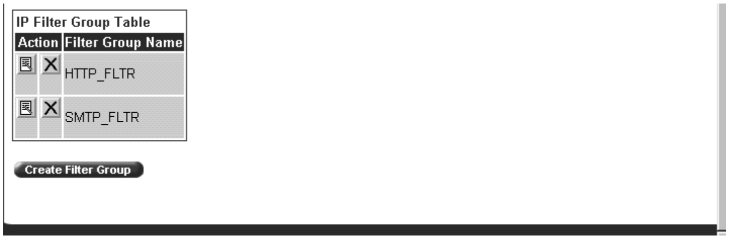
Figure 157 IP Classification page (2 of 3)



IP Filter Creation

Destination Address	● Ignore ○ Network Address Network Address: 0.0.0.0 Subnet Mask: 0.0.0.0 ○ Host Address Host IP Address: 0.0.0.0
Source Address	● Ignore ○ Network Address Network Address: 0.0.0.0 Subnet Mask: 0.0.0.0 ○ Host Address Host IP Address: 0.0.0.0
DSCP	Ignore
IP Protocol	Ignore
Destination Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0
Source Layer4 Port	● Ignore ○ Preconfigured Port # TFTP ○ User Defined Port # 0

Figure 158 IP Classification page (3 of 3)



IP Filter Group Table

Action	Filter Group Name
	HTTP_FLTR
	SMTP_FLTR

Note: When you choose the Ignore value, the filter matches all criteria for that parameter.

Table 87 describes the items on the IP Filter Table and IP Filter Creation sections of the IP Classification page.

Table 87 IP Filter Table and Filter Creation sections page items

Section	Item and MIB association	Range	Description
IP Filter Table	Action	☒	Deletes the row. Note: You cannot delete a filter if it is referenced in a filter group.
	Instance		Displays unique identifier.
	Destination Address (qosIpAceDstAddr)	XXX.XXX.XXX.XXX	Displays the IP address to match against the packet's destination IP address.
	Destination Address Mask (qosIpAceDstAddrMask)	XXX.XXX.XXX.XXX	Displays the mask for the matching of the destination IP address. A zero bit in the mask means that the corresponding bit in the address always matches. One (1) bits must be left justified.
	Source Address (qosIpAceSrcAddr)	XXX.XXX.XXX.XXX	Displays the IP address to match against the packet's source IP address.
	Source Address Mask (qosIpAceSrcAddrMask)	XXX.XXX.XXX.XXX	Displays the mask for the matching of the source IP address. One (1) bits must be left justified.
	DSCP (qosIpAceDscp)	Ignore, Integer (0..63)	Displays the value that the DSCP in the packet must have and match this filter. This displays the DSCP value that this filter attempts to match.
	Protocol (qosIpAceProtocol)	TCP (6) UDP (17) ICMP (1) IGMP (2) RSVP (46) Ignore (0)	Displays the IP protocol to match against the packet's IP protocol field.
	Destination L4 Port (qosIpAceDstL4PortMin) (qosIpAceDstL4PortMax)	Integer (0.65535)	Displays the value that the packet's layer 4 destination port number must have and match this filter.
	Source L4 Port (qosIpAceSrcL4PortMin) (qosIpAceSrcL4PortMax)	Integer (0.65535)	Displays the value that the packet's layer 4 source port number must have and match this filter.
	Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
IP Filter Creation/ Destination Address	Ignore		Click if you want the filter to ignore the packet's destination IP address.
	Network Address	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's destination network address. Enter the IP address to match against the packet's destination IP address.
	Subnet Mask)	XXX.XXX.XXX.XXX	Enter the mask for the matching of the destination IP address. A zero bit in the mask means that the corresponding bit in the address always matches. One (1) bits must be left justified.

Table 87 IP Filter Table and Filter Creation sections page items (continued)

Section	**Item and MIB association**	**Range**	**Description**
	Host Address)	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's destination host IP address. Enter the IP address to match against the packet's destination IP address.
IP Filter Creation/ Source Address	Ignore		Click if you want the filter to ignore the packet's source IP address.
	Network Address	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's source network address. Enter the IP address to match against the packet's source IP address.
	Subnet Mask)	XXX.XXX.XXX.XXX	Enter the mask for the matching of the source IP address. One (1) bits must be left justified.
	Host Address)	XXX.XXX.XXX.XXX	Click if you want the filter to match the packet's source host IP address. Enter the IP address to match against the packet's source IP address.
IP Filter Creation/ DSCP	DSCP (qosIpAceDscp)	Ignore, Integer (0..63)	Choose the value that the DSCP in the packet must have and match this filter.
IP Filter Creation/ IP Protocol	Protocol (qosIpAceProtocol)	Ignore (0) TCP (6) UDP (17) ICMP (1) IGMP (2) RSVP (46)	Choose the IP protocol to match against the packet's IP protocol field.
IP Filter Creation/ Destination Layer4 Port	Ignore		Click if you want the filter to ignore the packet's layer 4 destination port.
	Preconfigured Port #	TFTP FTP TELNET SMTP HTTP HTTPS	Choose the value that the packet's layer 4 destination port number must have and match this filter.
	User Defined Port #	Integer	Enter the value that the packet's layer 4 destination port number must have and match this filter.
IP Filter Creation/ Source Layer4 Port	Ignore		Click if you want the filter to ignore the packet's layer 4 source port.
	Preconfigured Port #	TFTP FTP TELNET SMTP HTTP HTTPS	Choose the value that the packet's layer 4 source port number must have and match this filter.
	User Defined Port #	Integer	Enter the value that the packet's layer 4 source port number must have and match this filter.

2 In the IP Filter Creation section, type information in the text boxes, or select from a list.

3 Click Submit.

The new IP filter configuration appears in the IP Filter Table (Figure 156). This table displays all IP filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

➡ **Note:** An IP filter configuration is not modifiable. The filter must be deleted and then re-created.

Deleting an IP filter configuration

To delete an IP filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 164).

2 In the IP Filter Table, in the IP filter configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the IP filter configuration.
- Click Cancel to return to the IP Classification page without making changes.

➡ **Note:** You cannot delete a filter if it is referenced in a filter group.

Creating an IP filter group configuration

To create an IP filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 156).

Table 88 describes the items on the IP Filter Group section of the IP Classification page.

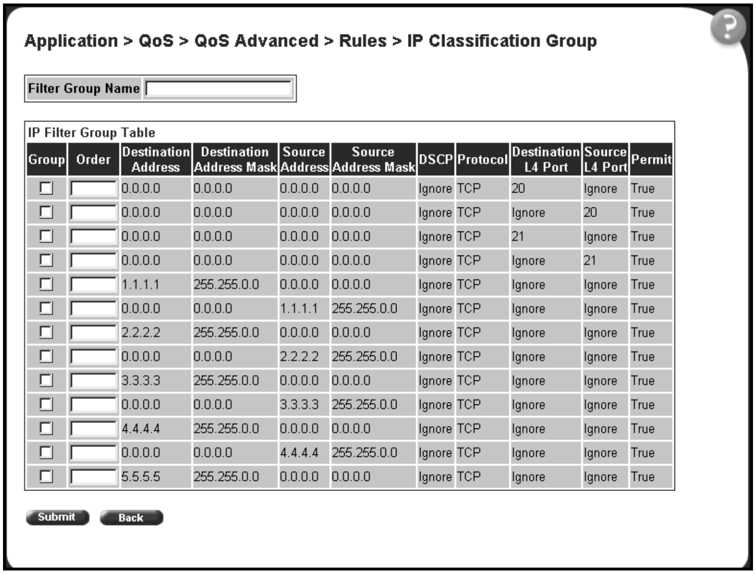
Table 88 IP Filter Group section page items

Item	**Description**
📝	Opens a modification page.
☒	Deletes the row.
Filter Group Name	A list of existing filter group configurations.
Create Filter Group	Opens a filter group creation page.

2 Click Create Filter Group.

The IP Classification Group page opens (Figure 159).This table displays all IP filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

Figure 159 IP Classification Group page



Application > QoS > QoS Advanced > Rules > IP Classification Group

Filter Group Name

IP Filter Group Table

Group	Order	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Port	Permit
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	20	Ignore	True
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	20	True
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	21	Ignore	True
☐		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	21	True
☐		1.1.1.1	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	1.1.1.1	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		2.2.2.2	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	2.2.2.2	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		3.3.3.3	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	3.3.3.3	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		4.4.4.4	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True
☐		0.0.0.0	0.0.0.0	4.4.4.4	255.255.0.0	Ignore	TCP	Ignore	Ignore	True
☐		5.5.5.5	255.255.0.0	0.0.0.0	0.0.0.0	Ignore	TCP	Ignore	Ignore	True

Table 89 describes the items on the IP Classification Group page.

Table 89 IP Classification Group page items

Item	Range	Description
Filter Group Name	1..16	Enter a character string to create an identity for the filter group configuration.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Type a number to establish the evaluation order of filters in the group.
Destination Address		The IP address that is matched against the packet's destination IP address.
Destination Address Mask		The mask for the matching of the destination IP address. Note: A zero bit in the mask means that the corresponding bit in the address always matches.
Source Address		The IP address that is matched against the packet's source IP address.
Source Address Mask		The mask for the matching of the source IP address.
DSCP		The value that the DSCP in the packet must have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP
Destination L4 Port		The value that the packet's layer 4 destination port number can have and match the filter entry.

Table 89 IP Classification Group page items

Item	**Range**	**Description**
Source L4 Port		The value that the packet's layer 4 source port number can have and match the filter entry.
Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3 Type information in the text boxes, or click the check box.

4 Click Submit.

The new configuration appears in the IP Filter Group Table (Figure 156).

Modifying an IP filter group configuration

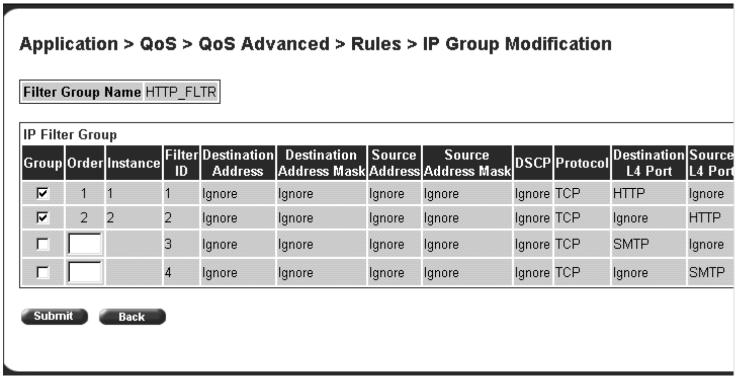
To modify an IP filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

The IP Classification page opens (Figure 156).

2 In the IP Filter Group Table section, in the IP filter group configuration of your choice, click the Modify icon.

The IP Group Modification page opens (Figure). This table displays all IP filter you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages. IP Group Modification page



Application > QoS > QoS Advanced > Rules > IP Group Modification

Filter Group Name HTTP_FLTR

IP Filter Group

Group	Order	Instance	Filter ID	Destination Address	Destination Address Mask	Source Address	Source Address Mask	DSCP	Protocol	Destination L4 Port	Source L4 Por
☑	1	1	1	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	HTTP	Ignore
☑	2	2	2	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	HTTP
☐			3	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	SMTP	Ignore
☐			4	Ignore	Ignore	Ignore	Ignore	Ignore	TCP	Ignore	SMTP

Table 90 describes the items on the IP Group Modification page.

Table 90 IP Modification Group page items

Item	Range	Description
Filter Group Name	1..16	Displays the name of the selected the filter group.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Displays the order for existing groups. Enter the desired order for the entries you are adding to the group.
Instance		Displays unique identifier.
Filter ID		Displays the filter identifier.
Destination Address		The IP address that is matched against the packet's destination IP address.
Destination Address Mask		The mask for the matching of the destination IP address. Note: A zero bit in the mask means that the corresponding bit in the address always matches.
Source Address		The IP address that is matched against the packet's source IP address.
Source Address Mask		The mask for the matching of the source IP address.
DSCP		The value that the DSCP in the packet must have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP
Destination L4 Port		The value that the packet's layer 4 destination port number can have and match the filter entry.
Source L4 Port		The value that the packet's layer 4 source port number can have and match the filter entry.

Table 90 IP Modification Group page items

Item	Range	Description
Permit	(1) True (2) False	If the frame matches the filter when this is set to true, the matching process stops.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3. Select (or deselect) the filter as a member of the Filter Group.
4. Click Submit.

Deleting an IP filter group configuration

To delete an IP filter group configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Rules > IP Classification.

   The IP Classification page opens (Figure 156).

2. In the IP Filter Group Table section, in the IP filter group configuration row of your choice, click the Delete icon.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the IP filter group configuration.
   - Click Cancel to return to the IP Classification page without making changes.

Note: You cannot delete a filter group that is referenced by a policy. You must first delete the policy.

Layer 2 filter and layer 2 filter group configurations

You can configure layer 2 filters by defining IEEE 802-based parameters, and selective layer 3 and layer 4 parameters. Layer 2 filter groups are defined by specifying the layer 2 filter to be included in the given filter group.

Beginning with software version 2.0, you can match up to 32 VLANs in one layer 2 filter.

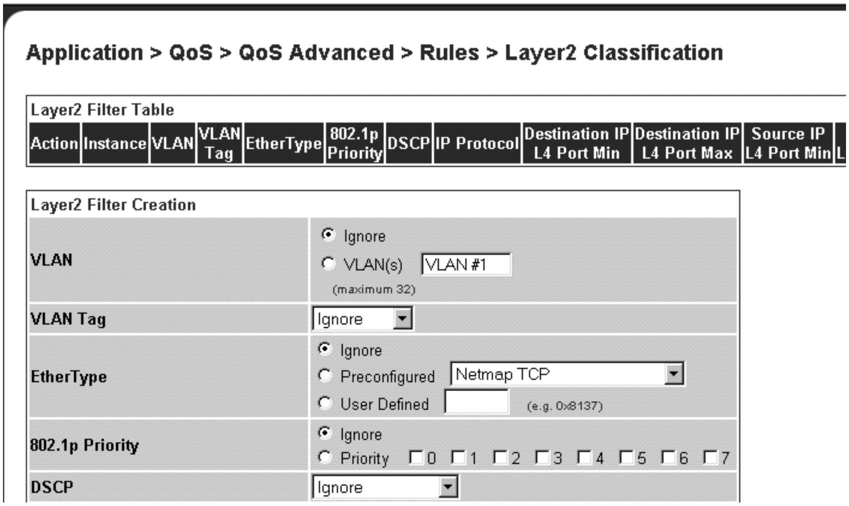
Creating a layer 2 filter configuration

To create a layer2 filter configuration:

1. From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

   The Layer2 Classification page opens (Figure 160, and Figure 161).

Figure 160 Layer2 Classification page (1 of 2)



Application > QoS > QoS Advanced > Rules > Layer2 Classification

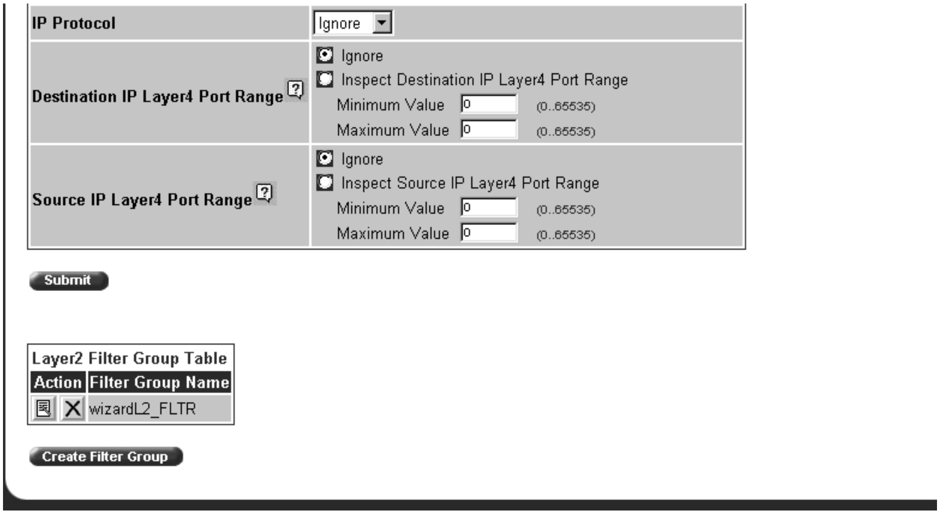
Layer2 Filter Table

Action	Instance	VLAN	VLAN Tag	EtherType	802.1p Priority	DSCP	IP Protocol	Destination IP L4 Port Min	Destination IP L4 Port Max	Source IP L4 Port Min	L

Layer2 Filter Creation

VLAN	● Ignore ○ VLAN(s) VLAN #1 (maximum 32)
VLAN Tag	Ignore
EtherType	● Ignore ○ Preconfigured Netmap TCP ○ User Defined (e.g. 0x8137)
802.1p Priority	● Ignore ○ Priority ☐0 ☐1 ☐2 ☐3 ☐4 ☐5 ☐6 ☐7
DSCP	Ignore

Figure 161 Layer2 Classification page (2 of 2)



IP Protocol	Ignore
Destination IP Layer4 Port Range	● Ignore ○ Inspect Destination IP Layer4 Port Range Minimum Value 0 (0..65535) Maximum Value 0 (0..65535)
Source IP Layer4 Port Range	● Ignore ○ Inspect Source IP Layer4 Port Range Minimum Value 0 (0..65535) Maximum Value 0 (0..65535)

Layer2 Filter Group Table

Action	Filter Group Name
☒	wizardL2_FLTR

Table 91 describes the items on the Layer2 Filter Table and Layer2 Filter Creation sections of the Layer2 Classification page.

Table 91 Layer2 Filter Table and Layer2 Filter Creation section items

Section	Item	Range	Description
Layer 2 Filter Table	Action	☒	Deletes the row.
	Instance		Displays unique identifier.
	VLAN	Ignore, 1-32	Click the VLANs you want to reference with this filer, up to 32 VLANs. Range is Ignore, 1 to 32.
	VLAN Tag	(1) Tagged (2) Untagged (3) Ignore	Displays whether or not to check VLAN tagging.

Table 91 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	**Item**	**Range**	**Description**
	EtherType	Ignore Netmap TCP Netmap XNS XTP LOOP Vines Vines IP Banyan Vines Echo Vines Banyan Echo ARP RARP IP IPv6 3Com NBP 3Com NBP Ack 3Com NBP ConnReq 3Com NBP ConnRsp 3Com NBP ConnComplt 3Com NBP CloseReq 3Com NBP CloseRsp 3Com NBP Datagram 3Com NBP Broadcast 3Com NBP NBP NameClaim 3Com NBP DelName LAP Atalk ARP Atalk IBM Net Mon IBMRT XNS Compatibility XNS IPX Netware SNMP User Defined	Displays the EtherType to match.
	802.1p Priority	Ignore, 0...7.	Displays the 802.1p priority level.
	DSCP	Ignore, Integer (0.63)	Displays the value that the DSCP in the packet must have and match this filter.

Table 91 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	Item	Range	Description
	IP Protocol	Ignore TCP UDP ICMP IGMP RSVP	Displays the IP protocol to match against the packet's IP protocol field.
	Destination IP L4 Port Min	Ignore, Integer (0.65535)	Displays the least value that the packet's layer 4 destination port number can have and match this filter.
	Destination IP L4 Port Max	Ignore, Integer (0.65535)	Displays the maximum value that the packet's layer 4 destination port number can have and match this filter.
	Source IP L4 Port Min	Ignore, Integer (0.65535)	Displays the least value that the packet's layer 4 source port number can have and match this filter.
	Source IP L4 Port Max	Ignore, Integer (0.65535)	Displays the maximum value that the packet's layer 4 source port number can have and match this filter.
Layer2 Filter Creation	VLAN	Ignore, 1-32	Choose up to 32 VLAN names or ID numbers.
	VLAN Tag	(1) Tagged (2) Untagged (3) Ignore	Choose whether or not to check VLAN tagging.

Table 91 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	**Item**	**Range**	**Description**
	EtherType	Ignore Netmap TCP Netmap XNS XTP LOOP Vines Vines IP Banyan Vines Echo Vines Banyon Echo ARP RARP IP IPv6 3Com NBP 3Com NBP Ack 3Com NBP ConnReq 3Com NBP ConnRsp 3Com NBP ConnComplt 3Com NBP CloseReq 3Com NBP CloseRsp 3Com NBP Datagram 3Com NBP Broadcast 3Com NBP NBP NameClaim 3Com NBP DelName LAP Atalk ARP Atalk IBM Net Mon IBMRT XNS Compatibility XNS IPX Netware SNMP User Defined	Choose the EtherType to match. Note: If you choose User Defined, enter the value.
	802.1p Priority	Ignore, 0...7.	Click the 802.1p priority level.
	DSCP	Ignore, Integer (0..63)	Choose the value that the DSCP in the packet must have and match this filter.

Table 91 Layer2 Filter Table and Layer2 Filter Creation section items (continued)

Section	Item	Range	Description
	IP Protocol	Ignore TCP UDP ICMP IGMP RSVP	Select the IP protocol to match against the packet's IP protocol field.
	Destination IP L4 Port Range	Ignore, Min, Max	Choose Ignore or type the minimum value and the maximum value that the packet's layer 4 destination port number can have and match this filter.
	Source IP L4 Port Range	Ignore, Min, Max	Choose Ignore or type the minimum value and the maximum value that the packet's layer 4 source port number can have and match this filter.

2 Type the information in the text boxes, or select from a list.

3 Click Submit.

The new Layer2 filter configuration appears in the Layer2 Filter Table (Figure 160).

➡ **Note:** You cannot delete a filter if it is referenced in a filter group.

Deleting a layer 2 filter configuration

To delete a layer 2 filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 160). This table displays all layer 2 filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

2 In the Layer2 Filter Table, in the layer 2 filter configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the filter configuration.
- Click Cancel to return to the Layer2 Classification page without making changes.

Note: A Layer 2 filter configuration cannot be modified. The configuration must be deleted and then recreated.

Creating a layer 2 filter group configuration

To create a Layer 2 filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 160).This table displays all layer 2 filters you created, using QoS wizard, Qos Quick Config, or QoS Advanced pages.

Table 92 describes the items on the Layer2 Filter Group Table section of the Layer2 Classification page.

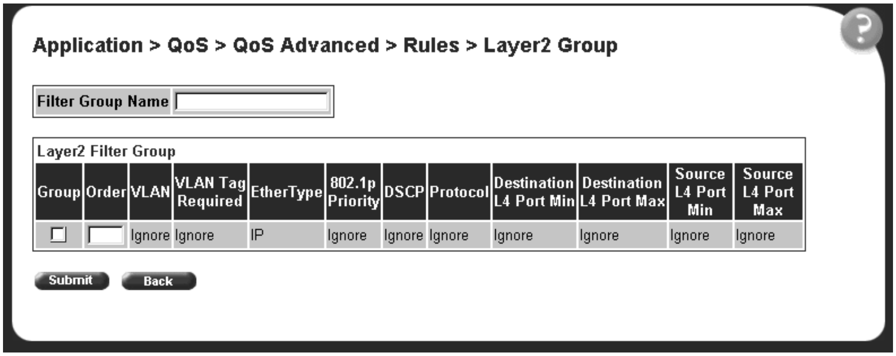
Table 92 IP Filter Group Table section items

Item	**Description**
📝	Opens a modification page.
☒	Deletes the row.
Filter Group Name	Lists existing filter group configurations.
Create Filter Group	Opens a filter group creation page.

2 Click Create Filter Group.

The Layer2 Group page opens (Figure 162).

Figure 162 Layer2 Group page



Application > QoS > QoS Advanced > Rules > Layer2 Group

Filter Group Name

Layer2 Filter Group

Group	Order	VLAN	VLAN Tag Required	EtherType	802.1p Priority	DSCP	Protocol	Destination L4 Port Min	Destination L4 Port Max	Source L4 Port Min	Source L4 Port Max
☐		Ignore	Ignore	IP	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore

Table 93 describes the items on the Layer2 Group page.

Table 93 Layer2 Group page items

Item	Range	Description
Filter Group Name	1..16	Enter a character string to create an identity for the filter group configuration.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Enter a number to establish the evaluation order of filters in the group.
VLAN		The VLAN ID(s) specified when the layer 2 filter was created.
VLAN Tag Required		The VLAN tag requirement option selected when the filter was created.
EtherType		The EtherType selected when the filter was created.
802.1p Priority		The 802.1p priority selected when the filter was created.
DSCP		The value that the DSCP in the packet can have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP.
Destination L4 Port Min		The least value that the packet's layer 4 destination port number can have and match this filter.
Destination L4 Port Max		The maximum value that the packet's layer 4 destination port number can have and match this filter.
Source L4 Port Min		The least value that the packet's layer 4 source port number can have and match this filter.

Table 93 Layer2 Group page items

Item	**Range**	**Description**
Source L4 Port Max		The maximum value that the packet's layer 4 source port number can have and match this filter.
	Note: To group multiple filters in a single group, assign Filter Index and Filter Order the same filter group name.	

3. Type information in the text boxes, or click the check box.
4. Click Submit.

   The new layer 2 filter group configuration appears in the Layer 2 Filter Group Table (Figure 160). This table displays all Layer 2 filters you created with QoS Wizard, QoS Quick Config, and QoS Advanced.

Modifying a layer 2 filter group configuration

To modify a layer 2 filter group configuration:

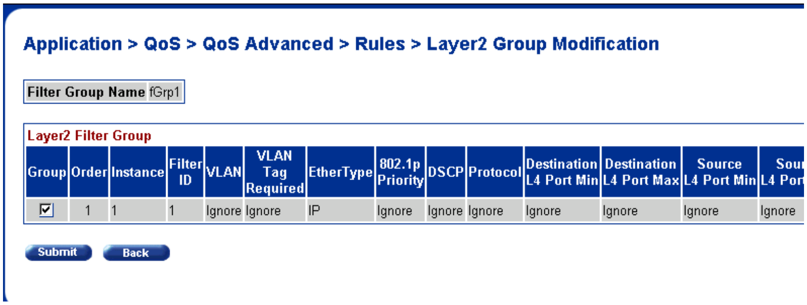
1. From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

   The Layer2 Classification page opens (Figure 160).

2. In the Layer2 Filter Group Table section, in the layer 2 filter group configuration of your choice, click the Modify icon.

   The Layer2 Group modification page opens (Figure 163).This table displays all Layer 2 Filter Groups you created with QoS Wizard, QoS Quick Config, and QoS Advanced.

Figure 163 Layer2 Group modification page



Application > QoS > QoS Advanced > Rules > Layer2 Group Modification

Filter Group Name fGrp1

Layer2 Filter Group

Group	Order	Instance	Filter ID	VLAN	VLAN Tag Required	EtherType	802.1p Priority	DSCP	Protocol	Destination L4 Port Min	Destination L4 Port Max	Source L4 Port Min	Sou L4 Por
☑	1	1	1	Ignore	Ignore	IP	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore	Ignore

Table 94 describes the items on the Layer2 Group modification page.

Table 94 Layer2 Group modification page items

Item	Range	Description
Filter Group Name	1..16	Displays the filter group name.
Group		Select (or deselect) the filter from membership in the filter group.
Order	Integer	Enter a number to establish the evaluation order of filters in the group.
Instance		Displays a unique identifier.
Filter ID		Displays the filter identifier.
VLAN		The VLAN ID(s) specified when the layer 2 filter was created.
VLAN Tag Required		The VLAN tag requirement option selected when the filter was created.
EtherType		The EtherType selected when the filter was created.
802.1p Priority		The 802.1p priority selected when the filter was created.
DSCP		The value that the DSCP in the packet can have and match this filter.
Protocol		The IP protocol that is matched against the packet's IP protocol field. The options are: Ignore, TCP, UDP, ICMP, IGMP, or RSVP.
Destination L4 Port Min		The least value that the packet's layer 4 destination port number can have and match this filter.
Destination L4 Port Max		The maximum value that the packet's layer 4 destination port number can have and match this filter.
Source L4 Port Min		The least value that the packet's layer 4 source port number can have and match this filter.
Source L4 Port Max		The maximum value that the packet's layer 4 source port number can have and match this filter.

3 Type information in the text boxes, or click the check box.

4 Click Submit.

Deleting a layer 2 filter group configuration

To delete a layer 2 filter group configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Rules > Layer2 Classification.

The Layer2 Classification page opens (Figure 160).

2 In the Layer2 Filter Group Table section, in the layer 2 filter group configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the filter group configuration.
- Click Cancel to return to the Layer2 Classification page without making changes.

Note: You cannot delete a filter group that is referenced by a policy. You must first delete the policy.

Configuring QoS actions

When you create a filter action, you specify the actions to be associated with specific IP and IEEE 802 filter groups. An action specifies the type of behavior you want a policy to apply to a flow of packets. When the filters match the incoming packets, the created actions are performed on those packets.

Creating a filter action configuration

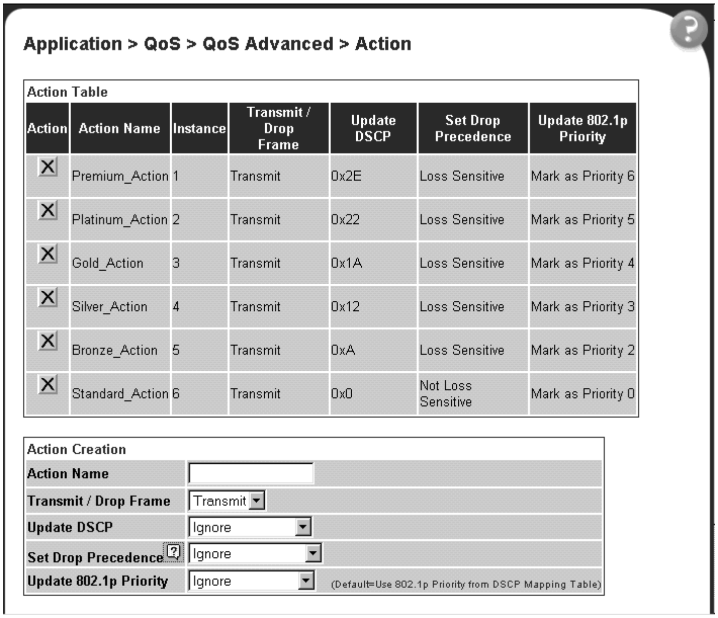
To create a filter action configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Actions.

The Action page opens (Figure 164).

Note: Beginning with software version 2.0, there are default actions for each service class.

Figure 164 Action page



Application > QoS > QoS Advanced > Action

Action Table

Action	Action Name	Instance	Transmit / Drop Frame	Update DSCP	Set Drop Precedence	Update 802.1p Priority
☒	Premium_Action	1	Transmit	0x2E	Loss Sensitive	Mark as Priority 6
☒	Platinum_Action	2	Transmit	0x22	Loss Sensitive	Mark as Priority 5
☒	Gold_Action	3	Transmit	0x1A	Loss Sensitive	Mark as Priority 4
☒	Silver_Action	4	Transmit	0x12	Loss Sensitive	Mark as Priority 3
☒	Bronze_Action	5	Transmit	0xA	Loss Sensitive	Mark as Priority 2
☒	Standard_Action	6	Transmit	0x0	Not Loss Sensitive	Mark as Priority 0

Action Creation

Action Name		
Transmit / Drop Frame	Transmit	
Update DSCP	Ignore	
Set Drop Precedence	Ignore	
Update 802.1p Priority	Ignore	(Default=Use 802.1p Priority from DSCP Mapping Table)

Table 95 describes the items on the Action page.

Table 95 Action page items

Item and MIB association	Range	Description
☒		Deletes the row.
Action Name	1..16	Type a character string to uniquely identify the action configuration.
Instance		Displays the unique identifier.
Transmit/Drop Frame (qosActionDrop)	(1) Transmit (2) Drop	Choose whether the frame being evaluated should be dropped or transmitted by this attribute. The default setting is Transmit.
Update DSCP (qosActionUpdateDSCP)	Ignore or integer	Type a value. When this field is defined, it causes the value contained in the Differentiated Services (DS) field of an associated IP datagram to be updated with the value of this object. The default setting is Ignore.

Table 95 Action page items (continued)

Item and MIB association	Range	Description
Set Drop Precedence (ntnQosActionExtSetDropPrec)	(1) Ignore (2) Loss Sensitive (3) Not loss Sensitive (4) Use Defaults (5) Use Egress Map	Choose a packet drop precedence value. Note: Generally, low packet drop precedence receives preferential treatment The default setting is Use Defaults
Update 802.1p Priority (ntnQosActionExtUpdatePri)	(1) Ignore (2) Priority 0 (3) Priority 1 (4) Priority 2 (5) Priority 3 (6) Priority 4 (7) Priority 5 (8) Priority 6 (9) Priority 7 (10) Use Defaults (11) Use Egress Map	Choose the action attribute that causes the value contained in the 802.1p priority field to be updated based on the value of this object. The update priority range values are 0 (lowest priority) to 7 (highest priority). Note: Use Defaults=Use 802.1p priority from DSCP mapping table. The default setting is Use Defaults.

2 In the Action Creation section, type information in the text boxes, or select from a list

3 Click Submit.

The new filter action configuration appears in the Action Table (Figure 164).

Note: Actions are not modifiable. They must be deleted and re-created.

Deleting an action configuration

To delete an action configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Actions.

The Action page opens (Figure 164).

2 In the Action Table section, in the filter action configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the filter configuration.
- Click Cancel to return to the Action page without making changes.

Note: You cannot delete an action that is referenced by a meter. you must first delete the meter.

Configuring QoS meters

Using the QoS Advanced pages, you can create, view, or delete meters. If you do not want to meter the data in your flow, go to "Configuring QoS shapers" on page 294.

Creating a meter

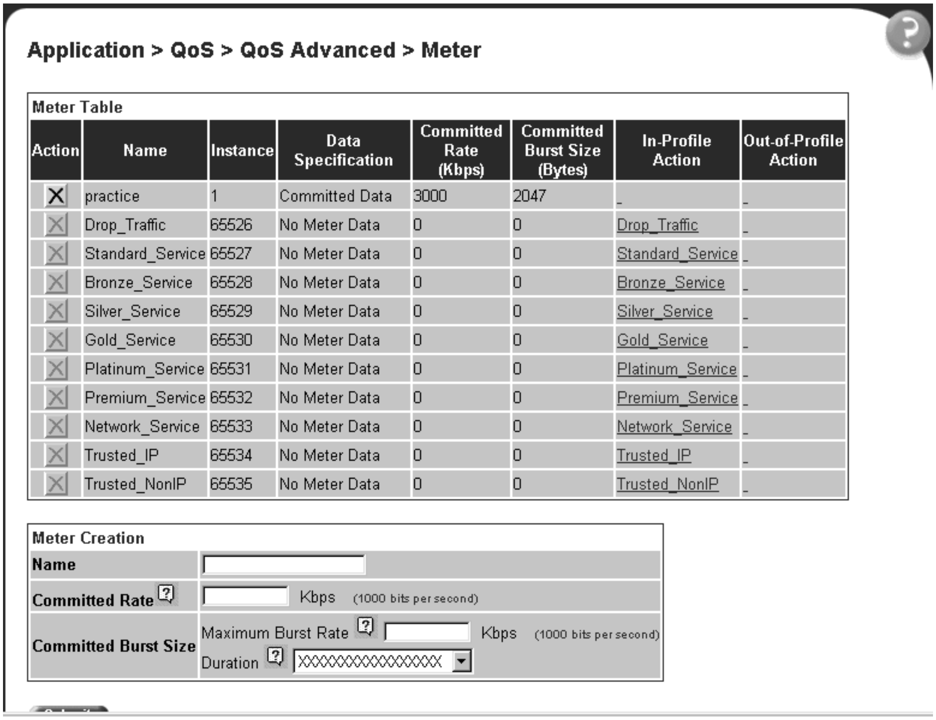
To create a meter:

1 From the main menu, choose Application > QoS > QoS Advanced > Meters.

The Qos Advanced Meter page opens (Figure 165). This table displays all meters you created with QoS Wizard, QoS Quick Config, and QoS Advanced.

Note: Beginning with software version 2.0, there are default meters for each service class.

Figure 165 QoS Advanced Meter page



Application > QoS > QoS Advanced > Meter

Meter Table

Action	Name	Instance	Data Specification	Committed Rate (Kbps)	Committed Burst Size (Bytes)	In-Profile Action	Out-of-Profile Action
☒	practice	1	Committed Data	3000	2047	_	_
☒	Drop_Traffic	65526	No Meter Data	0	0	Drop_Traffic	_
☒	Standard_Service	65527	No Meter Data	0	0	Standard_Service	_
☒	Bronze_Service	65528	No Meter Data	0	0	Bronze_Service	_
☒	Silver_Service	65529	No Meter Data	0	0	Silver_Service	_
☒	Gold_Service	65530	No Meter Data	0	0	Gold_Service	_
☒	Platinum_Service	65531	No Meter Data	0	0	Platinum_Service	_
☒	Premium_Service	65532	No Meter Data	0	0	Premium_Service	_
☒	Network_Service	65533	No Meter Data	0	0	Network_Service	_
☒	Trusted_IP	65534	No Meter Data	0	0	Trusted_IP	_
☒	Trusted_NonIP	65535	No Meter Data	0	0	Trusted_NonIP	_

Meter Creation

Name	
Committed Rate	Kbps (1000 bits per second)
Committed Burst Size	Maximum Burst Rate Kbps (1000 bits per second) Duration XXXXXXXXXXXXXXXXX

2 In the Meter Creation area, create the meter.

Table 96 describes the fields in the Meter Creation area, which you use to set new meters.

Table 96 Meter Creation fields

Item	Range	Description
Name	1 to 16 alphanumeric characters with no spaces	Enter the name for the meter you are creating.
Committed Rate	13 - 1,700,000 Kbps	Enter the Committed Rate in Kbps here.
Committed Burst Size	2,047 to 131,071 bytes Up to 7 durations	Maximum Burst Rate—Enter the Maximum Burst Rate in bytes. Duration—From the pull-down menu, choose 1 of up to 7 durations for the period that the Maximum Burst Rate is allowed.

3 Click Submit.

4 If you have not already specified the interface assignments, choose Applications > QoS > QoS Advanced > Devices > Interface Configuration page to connect the desired ports to the desired filters.

Note: Meter configurations are not modifiable. They must be deleted and the information re-entered.

Viewing meters

To view a meter:

1 From the main menu, choose Application > QoS > QoS Advanced > Meters.

The QoS Advanced Meters page opens (Figure 165).

2 View created meters in the Meter Table.

Table 97 describes the fields in the Meter Table area.

Table 97 Meter Table fields

Item	**Range**	**Description**
Action	☒	Deletes the meter.
Name		Displays the name of the meter.
Instance		Displays the unique identifier.
Data Specification	(1) No Meter Data (2) Metered Data	Displays whether the meter has metered data or not. (All meters created with software version 2.0 or higher have only metered data.)
Committed Rate	13 - 1,700,000 Kbps	Displays the Committed Rate in kbps.
Committed Burst Size	2,047 to 131,071 bytes	Displays the Committed Burst Size in bytes.
In-Profile Action	Configured, user-defined action	Displays the In-Profile Action for this meter.
Out-Profile Action	Configured, user-defined action	With a meter using metered data, this field displays the action specified for traffic that is out-of-profile. With a meter using no metered data, this field displays N/A. (All meters created with software version 2.0 or higher have only metered data.)

Deleting a meter

To delete a meter:

1. From the main menu, choose Application > QoS > QoS Advanced > Meters.

   The Meter page opens (Figure 165).

2. In the Meter Table section, click the Delete icon to delete the meter.

   A message opens prompting you to confirm your request.

3. Do one of the following:
   - Click Yes to delete the meter configuration.
   - Click Cancel to return to the Meter page without making changes.

➡ **Note:** You cannot delete a meter that is referenced by a policy. You must delete the policy first.

Configuring QoS shapers

➡ **Note:** You must be using either the BPS2000-1GT, BPS2000-2GT, or BPS2000-2GE MDA with the Business Policy Switch in order to implement the QoS shaping features.

Using the QoS Advanced pages, you can create, view, or delete shapers. If you do not want to shape the data in your flow, go to "Configuring QoS policies" on page 297.

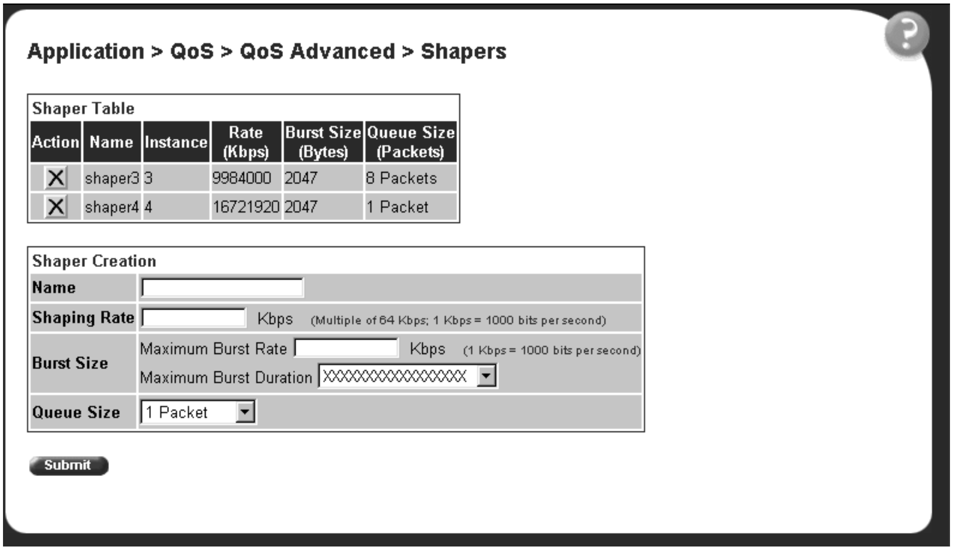
Creating a shaper

To create a shaper:

1 From the main menu, choose Application > QoS > QoS Advanced > Shapers.

The Qos Advanced Shapers page opens (Figure 166). All Shapers, including those created using the QoS Wizard and Qos Quick Config pages, display on this page.

Figure 166 QoS Advanced Shapers page



Application > QoS > QoS Advanced > Shapers

Shaper Table

Action	Name	Instance	Rate (Kbps)	Burst Size (Bytes)	Queue Size (Packets)
☒	shaper3	3	9984000	2047	8 Packets
☒	shaper4	4	16721920	2047	1 Packet

Shaper Creation

Name	
Shaping Rate	Kbps (Multiple of 64 Kbps; 1 Kbps = 1000 bits per second)
Burst Size	Maximum Burst Rate Kbps (1 Kbps = 1000 bits per second) Maximum Burst Duration XXXXXXXXXXXXXXXXX
Queue Size	1 Packet

2 In the Shaper Creation area, create the shape.

Table 96 describes the fields in the Shaper Creation area, which you use to set new shapers.

Table 98 Shaper Creation fields

Item	Range	Description
Name	1 to 16 alphanumeric characters with no spaces	Enter the name for the shaper you are creating.
Shaping Rate	1 - 4294967296	Enter the Shaping Rate in Kbps here. This is the maximum rate at which traffic shaped using this shaper will be transmitted over a given duration. Note: The system rounds up the shaping rate you enter to a multiple of 64 Kbps.

Table 98 Shaper Creation fields (continued)

Item	**Range**	**Description**
Burst Size	6 durations	Maximum Burst Rate—Enter the Maximum Burst Rate in Kbps. This determines the maximum traffic burst size that can be transmitted without a shaping delay. Duration—From the pull-down menu, choose 1 of the 6 durations for the period that the Maximum Burst Rate is allowed.
Queue Size	1, 2, 4, 8, or 16 packets	Choose the queue depth from the pull-down menu. This is the number of packets that can exceed the traffic burst size and still be queued for transmission.

3 Click Submit.

Note: Shaper configurations are not modifiable. They must be deleted and the information re-entered.

Viewing shapers

To view a shaper:

1 From the main menu, choose Application > QoS > QoS Advanced > Shapers.

The QoS Advanced Shapers page opens (Figure 165).

2 View created shapers in the Shaper Table. This table displays all the shapers you configured, including those with QoS Wizard and QoS Quick Config.

Table 99 describes the fields in the Shaper Table area.

Table 99 Shaper Table fields

Item	**Range**	**Description**
Action	☒	Deletes the shaper.
Name		Displays the name of the shaper.
Instance		Displays the unique identifier.
Rate	1 - 4294967296	Displays the maximum rate at which traffic shaped using this shaper will be transmitted over a given duration. Displays the rate rounded up to multiples of 64 Kbps.

Table 99 Shaper Table fields (continued)

Item	Range	Description
Burst Size		Displays the maximum traffic burst size that can be transmitted without a shaping delay. Calculated internally using the configured Maximum Burst Rate and Maximum Burst Duration.
Queue Size	1, 2, 4, 8, or 16 packets	Displays the number of packets that can exceed the traffic burst size and still be queued for transmission.

Deleting a shaper

To delete a shaper:

1 From the main menu, choose Application > QoS > QoS Advanced > Shapers.

The Qos Advanced Shaper page opens (Figure 166).

2 In the Shaper Table section, click the Delete icon to delete the shaper.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the shaper configuration.
- Click Cancel to return to the Shaper page without making changes.

➡ **Note:** You cannot delete a shaper that is referenced by a policy. You must delete the policy first.

Configuring QoS policies

You can configure QoS policies by creating filters in the hardware that apply a set of packet filtering criteria and actions to individual interfaces.

If you want to meter your data, you must reference both an In-Profile action and an Out-Profile action. The In-Profile action directs the switch how to handle the data flow that is within the meter you set (refer to "Configuring QoS meters"), and the Out-Profile directs the switch how to handle all other data.

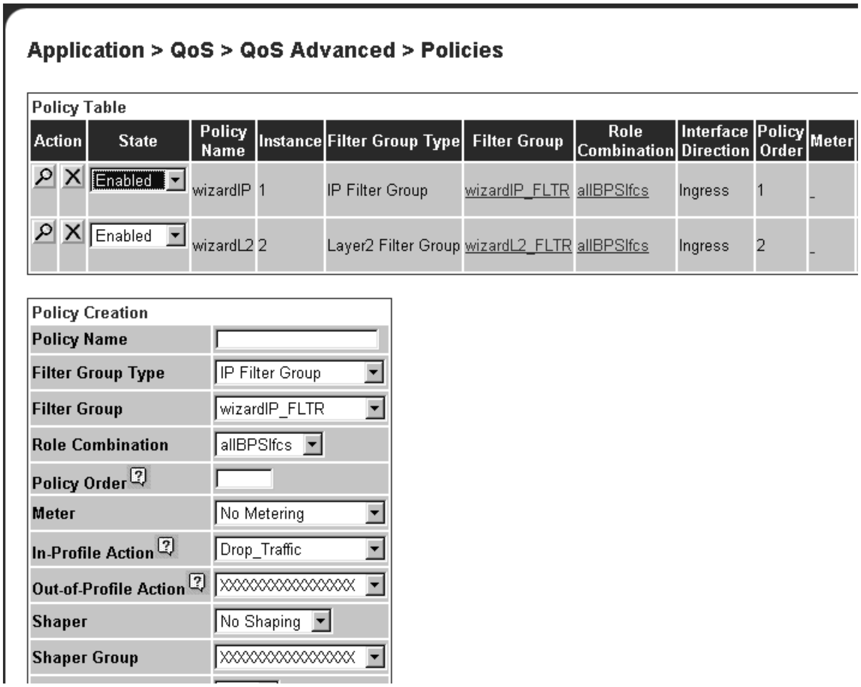
Installing defined filters

To create a hardware policy filter configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The QoS Advanced Policies page opens (Figure 167, Figure 168, and Figure 169). This table displays all configured policies, including ones created with QoS Wizard and QoS Quick Config.

Figure 167 QoS Advanced Policies page (1 of 3)



Application > QoS > QoS Advanced > Policies

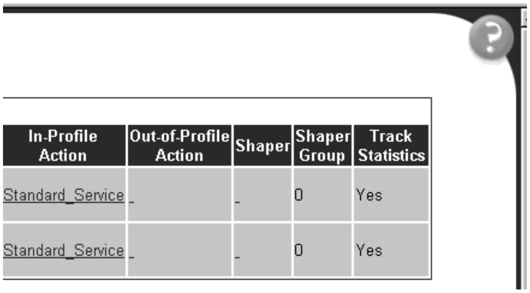
Policy Table

Action	State	Policy Name	Instance	Filter Group Type	Filter Group	Role Combination	Interface Direction	Policy Order	Meter
🔍 ✕	Enabled	wizardIP	1	IP Filter Group	wizardIP_FLTR	allBPSIfcs	Ingress	1	_
🔍 ✕	Enabled	wizardL2	2	Layer2 Filter Group	wizardL2_FLTR	allBPSIfcs	Ingress	2	_

Policy Creation

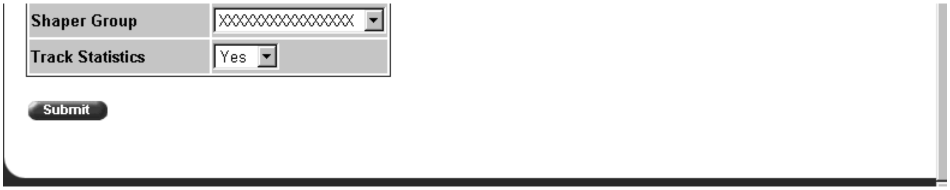
Policy Name	
Filter Group Type	IP Filter Group
Filter Group	wizardIP_FLTR
Role Combination	allBPSIfcs
Policy Order	
Meter	No Metering
In-Profile Action	Drop_Traffic
Out-of-Profile Action	XXXXXXXXXXXXXXX
Shaper	No Shaping
Shaper Group	XXXXXXXXXXXXXXX

Figure 168 QoS Advanced Policies page (2 of 3)



In-Profile Action	Out-of-Profile Action	Shaper	Shaper Group	Track Statistics
Standard_Service	_	_	0	Yes
Standard_Service	_	_	0	Yes

Figure 169 QoS Advanced Policies page (3 of 3)



Shaper Group	XXXXXXXXXXXXXXX
Track Statistics	Yes

Table 100 describes the items on the QoS Advanced Policy page.

Table 100 Policy page items

Section	Item and MIB association	Range	Description
Policy Table	Action	🔍	Opens a view only statistics table. The table displays current filter statistics in bytes and packets.
		☒	Deletes the row.
	State	(1) Enabled (2) Disabled	Enables or disables the policy.
	Policy Name	1..16	A list of the names of existing target configurations.
	Instance		Displays the unique identifier.
	Filter Group Type		The type of filter group that is referenced by this instance of the Target class. The options are: IP Filter Group or Layer2 Filter Group.
	Filter Group		The filter group that is associated with this target.
	Role Combination		The interfaces to which this target specification applies, specified in terms of a role combination tag.
	Interface Direction		The direction of packet flow at the interface to which this target specification applies.
	Policy Order		The number used to determine the order of precedence for this target specification.
	Meter		The meter associated with this entry, if there is one.
	In-Profile Action		Displays the name of the In-Profile action for this policy.
	Out-of-Profile Action		Displays the name of the Out-of-Profile action for this policy. This field applies only to metered data.
	Shaper		Displays the name of the shaper for this policy, if there is one
	Shaper Group	2 - 63	Displays the shaper group ID for this policy.
	Track Statistics		Displays whether you are tracking statistics for this policy.
Policy Creation	Policy Name	1..64	Type a character string to create a unique name to identify this policy.
	Filter Group Type (qosTargetAclType)	(1) IP Filter Group (2) Layer2 Filter Group	Choose the type of filter group to associate with this policy.

Table 100 Policy page items

Section	Item and MIB association	Range	Description
	Filter Group		Choose the filter group to associate with this policy.
	Role Combination (qosTargetInterfaceRoles)		Choose the type of interface to which this policy applies, specified in terms of a role combination.
	Policy Order (qosTargetOrder)	Integer	Enter a number to use as a determinate of the order of precedence for this filter.
	Meter (qosTargetMeter)		Choose the meter associated with this entry.
	In-Profile Action (qosTargetInProfileIAction)		Choose the action you want to take for the data associated with this policy.
	Out-of-Profile Action (qosTargetOutOfProfileIAction)		Choose the action you want to take associated with this policy for metered data that is not within the configured profile.
	Shaper (qosTargetShaping Params)		Choose the shaper, if any, to apply to this policy
	Shaper Group (qosTargetShapingGroup)	2- 63	Choose the shaper group, if any, to apply to this policy.
	Track Statistics (ntnQosTargetStatsTrack Statistics)	(1) Yes (2) No	Choose whether or not to track statistics for policy.

2 Complete the fields as described.

3 Click Submit.

Note: Beginning with software version 2.0, you can enable or disable a policy. The default setting is Enabled.

Viewing hardware policy statistics

To view statistics for a selected hardware policy configuration:

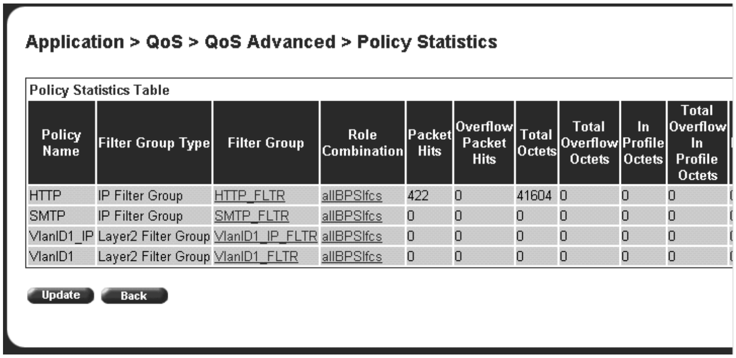
1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The QoS Advanced Policies page opens (Figure 167).

2 In the Policy Table section, in the filter group configuration of your choice, click the View icon.

The Policy Statistics page opens (Figure 170).

Figure 170 Policy Statistics page



Application > QoS > QoS Advanced > Policy Statistics

Policy Statistics Table

Policy Name	Filter Group Type	Filter Group	Role Combination	Packet Hits	Overflow Packet Hits	Total Octets	Total Overflow Octets	In Profile Octets	Total Overflow In Profile Octets
HTTP	IP Filter Group	HTTP_FLTR	allBPSIfcs	422	0	41604	0	0	0
SMTP	IP Filter Group	SMTP_FLTR	allBPSIfcs	0	0	0	0	0	0
VlanID1_IP	Layer2 Filter Group	VlanID1_IP_FLTR	allBPSIfcs	0	0	0	0	0	0
VlanID1	Layer2 Filter Group	VlanID1_FLTR	allBPSIfcs	0	0	0	0	0	0

Table 101 describes the items on the Policy Statistics page.

Table 101 Policy Statistics page items

Item and MIB association	Description
Policy Name	The name of the selected policy.
Filter Group Type	The type of group that is referenced by this instance of the filter policy class. The options are: IP Filter Group or Layer2 Filter Group.
Filter Group	The filter group associated with the selected policy.
Role Combination	The interfaces to which this policy applies, specified in terms of a role combination.
Packet Hits (ntnQosTargetStatsPkHits)	The packets selected for additional processing. The action taken is based on a match with specified filter and/or threshold information.
Overflow Packet Hits (ntnQosTargetStatsOverflowPkHits)	The number of times the associated ntnQosTargetStatsPktHits counter overflowed.
Total Octets (ntnQosTargetStatsTotalOctets)	The total number of octets associated with packet hits for this policy.
Total Overflow Octets (ntnQosTargetStatsTotalOverflowOctets)	The total number of times the associated ntnQosTargetStatsTotalOctets counter overflowed.
In Profile Octets (ntnQosTargetStatsTotalInProfOctets)	The total number of in-profile octets associated with packet hits for this policy.

Table 101 Policy Statistics page items (continued)

Item and MIB association	Description
Overflow In Profile Octets (ntnQosTargetStatsTotalInProfOverflowOctets)	The number of times the associated ntnQosTargetStatsTotalInProfOctets counter overflowed.
Out Profile Octets (ntnQosTargetStatsTotalOutProfOctets)	The total number of out-of-profile octets associated with packet hits for this policy.
Overflow Out Profile Octets (ntnQosTargetStatsTotalOutProfOverflowOctets)	The number of times the associated ntnQosTargetStatsTotalOutProfOctets counter overflowed.
Shaping Q Drops (ntnQosTargetStatsShapingQDrops)	The total number of octets dropped from the shaping queues for this policy.
Overflow Shaping Q Drops (ntnQosTargetStatsOverflowShapingQDrops)	The number of times the associated ntnQosTargetStatsShapingQDrops counter overflowed.

3 To refresh the hardware policy statistics, click Update.

Deleting a hardware policy configuration

To delete a hardware policy configuration:

1 From the main menu, choose Application > QoS > QoS Advanced > Policies.

The QoS Advanced Policies page opens (Figure 167).

2 In the Policy Table section, in the hardware policy configuration row of your choice, click the Delete icon.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the hardware policy configuration.
- Click Cancel to return to the Policy page without making changes.

Configuring QoS Policy Agent (QPA) characteristics

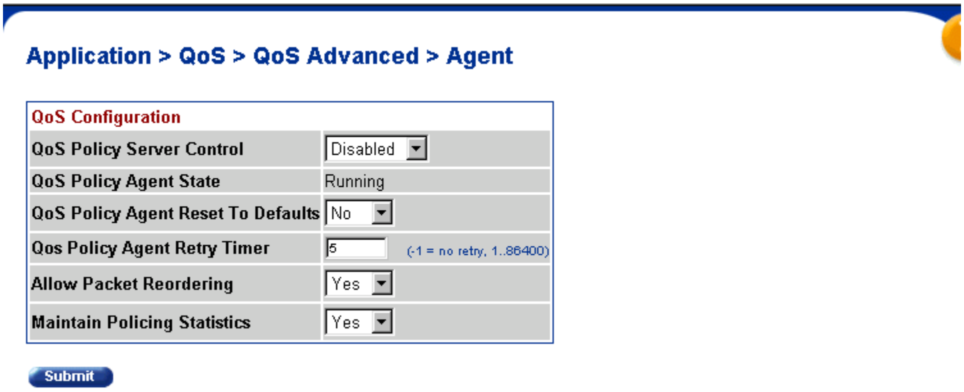
You can configure QPA operational parameters.

To open the Agent page:

1 From the main menu, choose Application > QoS > QoS Advanced > Agent.

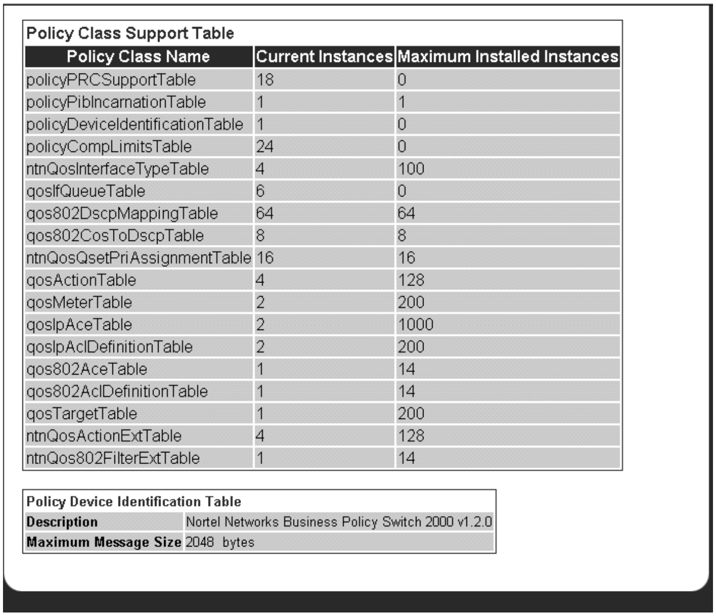
The Agent page opens (Figure 171 and Figure 172).

Figure 171 Agent page (1 of 2)



QoS Configuration	
QoS Policy Server Control	Disabled
QoS Policy Agent State	Running
QoS Policy Agent Reset To Defaults	No
Qos Policy Agent Retry Timer	5 (-1 = no retry, 1..86400)
Allow Packet Reordering	Yes
Maintain Policing Statistics	Yes

Figure 172 Agent page (2 of 2)



Policy Class Support Table

Policy Class Name	Current Instances	Maximum Installed Instances
policyPRCSupportTable	18	0
policyPibIncarnationTable	1	1
policyDeviceIdentificationTable	1	0
policyCompLimitsTable	24	0
ntnQosInterfaceTypeTable	4	100
qosIfQueueTable	6	0
qos802DscpMappingTable	64	64
qos802CosToDscpTable	8	8
ntnQosQsetPriAssignmentTable	16	16
qosActionTable	4	128
qosMeterTable	2	200
qosIpAceTable	2	1000
qosIpAclDefinitionTable	2	200
qos802AceTable	1	14
qos802AclDefinitionTable	1	14
qosTargetTable	1	200
ntnQosActionExtTable	4	128
ntnQos802FilterExtTable	1	14

Policy Device Identification Table

Description	Nortel Networks Business Policy Switch 2000 v1.2.0
Maximum Message Size	2048 bytes

Table 102 describes the items on the Agent page.

Table 102 Agent page items

Section	Item and MIB association	Range	Description
QoS Configuration	QoS Policy Server Control	Enabled Disabled	Choose to enable or disable the QoS Policy server control. Note: Choosing to enable COPS disables local policy control.
	QoS Policy Agent State (ntnQosConfigQpaState)	Running Initialized Disabled	The current status of the policy agent.
	QoS Policy Agent Reset to Defaults (ntnQosConfigQpaState)	(1) Yes (2) No	Choose whether or not to reset the policy agent to the default settings.
	QoS Policy Agent Retry Timer (ntnQosConfigQpaRetryTimer)	-1 = no retry, 1..86400	Type the time, in seconds, between the receipt of a connection termination/rejection indication and the start of a new connection request. Note: A value of -1 indicates that a connection retry should not be attempted after a failed attempt.

Table 102 Agent page items (continued)

Section	Item and MIB association	Range	Description
	Allow Packet Reordering (ntnQosConfigAllowPacketReordering)	(1) Yes (2) No	Support for certain PHBs requires that packets within a flow not be reordered when transmitted. Choose: • Yes—Allows full flexibility of assigning packet to egress queue. • No—Agent verifies that in-profile and out-of-profile actions associated with the flow do not cause packets from same flow to be assigned to different egress queues.
	Maintain Policing Statistics (ntnQosConfigMaintainPolicingStats)	(1) Yes (2) No	Policing statistics, such as in-profile and out-of-profile octets, are often important to evaluate the efficacy of the installed policies. Tracking these statistics uses additional system resources, which limits the amount of filters available for classification. Choose: • Yes—Tracks statistics for all policies defined after value is set. • No—Does not track statistics for new policies.
Policy Class Support Table	Policy Class Names		The name of the policy.
	Current Instances		The current class entries.
	Maximum Installed Instances		The maximum number of allowed class entries.
Policy Device Identification Table	Description		The system description.
	Maximum Message Size		The maximum target message size supported by the device.

2 In the QoS Configuration section, type information in the text boxes, or select from a list.

3 Click Submit.

Chapter 10
Implementing Common Open Policy Services (COPS)

Enabling COPS in your networks allows the policy server to:

- Gather all relevant information.
- Make a decision based on your (as network administrator) set policies and network resources,
- Communicate that decision in the form of proper service to the appropriate group or client (bandwidth, ACLs, QoS).

A solid COPS strategy is closely tied to Internet Protocol (IP) address management and network management.

This chapter discusses the COPS options available to you in the Web-based management interface.

The COPS options are:

- Viewing COPS statistics and capabilities (next)
- Creating COPS client configurations (page 312)

Viewing COPS statistics and capabilities

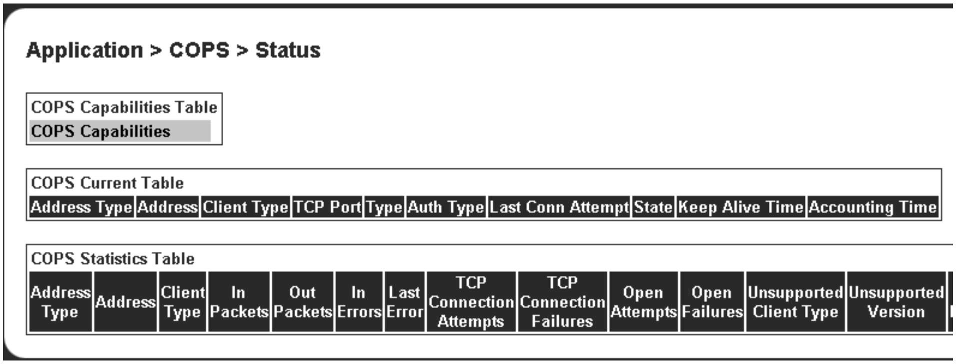
You can view a list of the capabilities of the COPS client to connect to a COPS server and view a table displaying the current status of all COPS server connections.

To view COPS capabilities and statistics:

1 From the main menu, choose Application > COPS > Status.

The Status page opens (Figure 173).

Figure 173 Status page



Application > COPS > Status

COPS Capabilities Table

COPS Capabilities

COPS Current Table

Address Type	Address	Client Type	TCP Port	Type	Auth Type	Last Conn Attempt	State	Keep Alive Time	Accounting Time

COPS Statistics Table

Address Type	Address	Client Type	In Packets	Out Packets	In Errors	Last Error	TCP Connection Attempts	TCP Connection Failures	Open Attempts	Open Failures	Unsupported Client Type	Unsupported Version

Table 103 describes the items on the Status page.

Table 103 Status page items

Section	Item	Descriptions
COPS Capabilities Table	COPS Capabilities	A list of COPS protocols supported by the Business Policy Switch 2000. The current supported version is COPSv1 protocol.
COPS Current Table	Address Type	The type of address in copsClientServerAddress.
	Address	The IPv4, IPv6, or DNS address of a COPS server.
	Client Type	The protocol client type for this entry. Note: Multiple client types can be served by a single COPS server. Note: The value 0 (zero) indicates that this entry contains information about the underlying connection.
	TCP Port	The TCP port number on the COPS server to which the client is connected.

Table 103 Status page items (continued)

Section	Item	Descriptions
COPS Current Table, cont.	Type	The indicator of the source of the COPS server information. Note: COPS servers can be configured by network management into copsClientServerConfigTable and appear in this entry with type copsServerStatic(1). Alternatively, the type, or entry, can be a notification from another COPS server by way of the COPS PDP-Redirect mechanism and appear as copsServerRedirect(2).
	Authorization Type	The indicator of the current security mode in use between the client and the COPS server.
	Last Conn Attempt	The timestamp of the last time the client attempted to connect to this COPS server.
	State	The operational state of the connection and COPS protocol with respect to this COPS server.
	Keep Alive Time	The value of the Keepalive timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates no keepalive activity is expected.
	Accounting Time	The value of the COPS protocol Accounting timeout, in centiseconds, currently in use by the client, as specified by the COPS server in the Client-Accept operation. Note: A value of 0 (zero) indicates that the client should not send any unsolicited accounting reports.
COPS Statistics Table	Address Type	The type of address in copsClientServerAddress.
	Address	The IPv4, IPv6, or DNS address of a COPS server.
	Client Type	The protocol client type for this entry. Note: Multiple client types can be served by a single COPS server. Note: The value 0 (zero) indicates that this entry contains information about the underlying connection.
	In Packets	The total number of COPS packets that the client has received from this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Out Packets	The total number of COPS packets that the client has sent to this COPS server marked for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	In Errors	The total number of COPS packets that the client has received from this COPS server marked for the selected client type that contained errors in syntax. Note: This is a cumulative value and *is not* zeroed on new connections.
	Last Error	The code contained in the last COPS protocol Error Object received by the client from this COPS server marked for the selected client type. Note: This value *is not* zeroed on COPS Client-Open operations.

Table 103 Status page items (continued)

Section	**Item**	**Descriptions**
COPS Statistics Table, cont.	TCP Connection Attempts	The number of times that the COPS client attempted to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
	TCP Connection Failures	The number of times that the COPS client failed to open a TCP connection to the COPS server. Note: This value is valid only for client type 0. Note: This is a cumulative value and *is not* zeroed on new connections.
	Open Attempts	The number of times that the COPS client attempted to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Open Failures	The number of times that the COPS client failed to perform a COPS Client-Open to a COPS server for the selected client type. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unsupported Client Type	The total number of COPS packets that this client has received from COPS servers that referred to client types that are unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unsupported Version	The total number of COPS packets that this client has received from COPS servers marked for the selected client type that had a COPS protocol version number that is unsupported by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Length Mismatch	The total number of COPS packets that the client received from COPS servers marked for the selected client type that had a COPS protocol message length that did not match the actual received packet. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unknown Opcode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Unknown Cnum	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Num not recognized by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Bad Ctype	The total number of COPS packets that the client received from COPS servers marked for the selected client type containing a COPS protocol object C-Type not defined for the C-Nums known by the client. Note: This is a cumulative value and *is not* zeroed on new connections.

Table 103 Status page items (continued)

Section	Item	Descriptions
COPS Statistics Table, cont.	Bad Sends	The total number of COPS packets that the client attempted to send to COPS servers marked for the selected client type that resulted in a transmit error. Note: This is a cumulative value and *is not* zeroed on new connections.
	Wrong Objects	The total number of COPS packets that the client received from COPS servers marked for the selected client type not containing a permitted set of COPS protocol objects. Note: This is a cumulative value and *is not* zeroed on new connections.
	Wrong OpCode	The total number of COPS packets that the client received from COPS servers marked for the selected client type having a COPS protocol Op Code that should not have been sent to a COPS client, for example, Open-Requests. Note: This is a cumulative value and *is not* zeroed on new connections.
	Timedout Clients	The total number of times that the client has been shut down for the selected client type by COPS servers that detected a COPS protocolKeepalive timeout. Note: This is a cumulative value and *is not* zeroed on new connections.
	Auth Failures	The total number of times that the client received a COPS packet marked for the selected client type that could not be authenticated using the authentication mechanism used by the client. Note: This is a cumulative value and *is not* zeroed on new connections.
	Auth Missing	The total number of times that the client received a COPS packet marked for this client type not containing authentication information.

Creating a COPS configuration

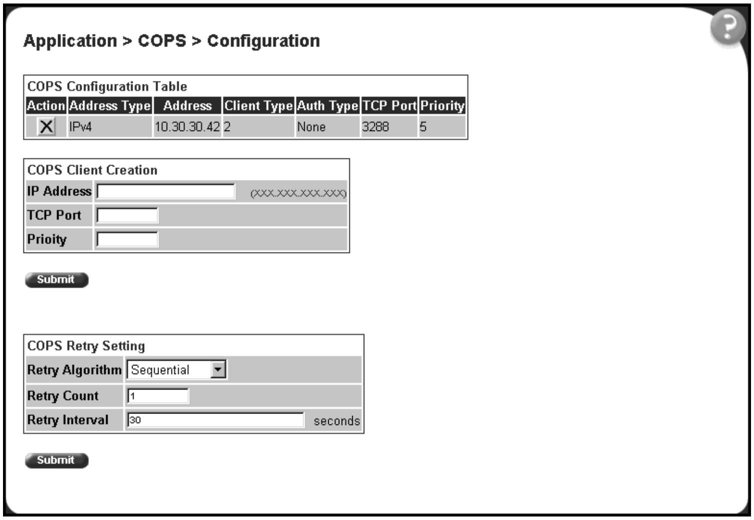
You can select the COPS server(s) to use to obtain policy information by creating COPS configurations.

To create a COPS configuration:

1. From the main menu, choose Application > COPS > Configuration.

   The Configuration page opens (Figure 174).

Figure 174 Configuration page



Application > COPS > Configuration

COPS Configuration Table

Action	Address Type	Address	Client Type	Auth Type	TCP Port	Priority
☒	IPv4	10.30.30.42	2	None	3288	5

COPS Client Creation

IP Address		(xxx.xxx.xxx.xxx)
TCP Port		
Prioity		

COPS Retry Setting

Retry Algorithm	Sequential	
Retry Count	1	
Retry Interval	30	seconds

Table 104 describes the items on the COPS Configuration Table section of the Configuration page.

Table 104 COPS Configuration Table section items

Section	Item	Range	Description
COPS Configuration Table	☒		Deletes the row.
	Address Type		The type of address in copsClientServerConfigAddress.
	Address		The IPv4, IPv6, or DNS address of the COPS server.
	Client Type		The COPS protocol client type this COPS server is capable of serving. Note: A single COPS server can serve multiple client types.

Table 104 COPS Configuration Table section items (continued)

Section	Item	Range	Description
COPS Configuration Table, cont.	Auth Type		The authentication mechanism for this COPS client to request when negotiating security at the start of a connection to a COPS server.
	TCP Port		The TCP port number on the COPS server.
	Priority		The level of priority assigned to the client. Note: When a COPS client attempts to contact COPS servers for the appropriate client type, it contacts higher numbers (priority) first. The order used for server entries with the same priority is undefined. COPS servers notified to the client using the COPS protocol PDP-Redirect mechanism are always processed with higher priority than any entries in this table.
COPS Client Creation	IP Address	XXX.XXX.XXX.XXX	The IP address of the COPS client.
	TCP Port	Integer	Type the TCP port number on the COPS server.
	Priority		Type a number that represents the level of priority. Note: When a COPS client attempts to contact COPS servers for the appropriate client type, it contacts higher numbers (priority) first. The order used for server entries with the same priority is undefined. COPS servers notified to the client using the COPS protocol PDP-Redirect mechanism are always processed with higher priority than any entries in this table.
COPS Retry Setting	Retry Algorithm	(1) Sequential (2) Round Robin	Choose the type of algorithm to use.
	Retry Count	Integer	Type the number of retry attempts.
	Retry Interval	Integer	Type, in seconds, the retry interval.

2 Type information in the text boxes, or select from a list.

Click Submit.

Note: COPS configurations are not modifiable. They must be deleted and the information recreated.

Deleting a COPS client configuration

To delete a COPS client configuration:

1 From the main menu, choose Application > COPS > Configuration.

The Configuration page opens (Figure 174).

2 In the COPS Configuration Table, click the Delete icon for the entry you want to delete.

A message opens prompting you to confirm your request.

3 Do one of the following:

- Click Yes to delete the configuration.
- Click Cancel to return to the Configuration page without making changes.

Chapter 11
Support menu

The customer support options available to you are:

- Help
- Release Notes
- Manuals
- Upgrade

Using the online help option

You can read information about management page functions in the online help menu embedded in the Web-based management interface.

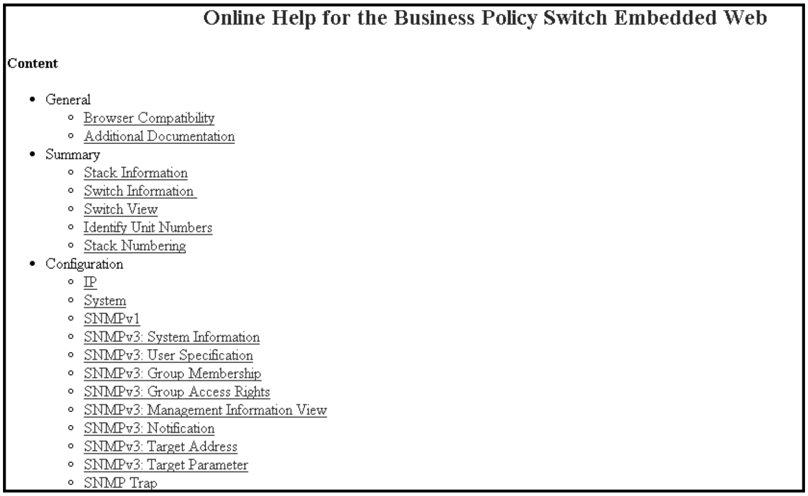
To open online help:

1 From the main menu, choose Support > Help or click the Help icon located in the upper right corner of any management page.

?

The Online Help menu opens in a separate Web browser (Figure 175).

Figure 175 Online help window



Online Help for the Business Policy Switch Embedded Web

Content

- General
  - Browser Compatibility
  - Additional Documentation
- Summary
  - Stack Information
  - Switch Information
  - Switch View
  - Identify Unit Numbers
  - Stack Numbering
- Configuration
  - IP
  - System
  - SNMPv1
  - SNMPv3: System Information
  - SNMPv3: User Specification
  - SNMPv3: Group Membership
  - SNMPv3: Group Access Rights
  - SNMPv3: Management Information View
  - SNMPv3: Notification
  - SNMPv3: Target Address
  - SNMPv3: Target Parameter
  - SNMP Trap

2 Click on any content item to read information about the topic (if you clicked the Help icon on a management page, information about that page is immediately displayed).

3 Click Return to Top to return to the Content index.

4 Close the Web browser

Downloading technical publications

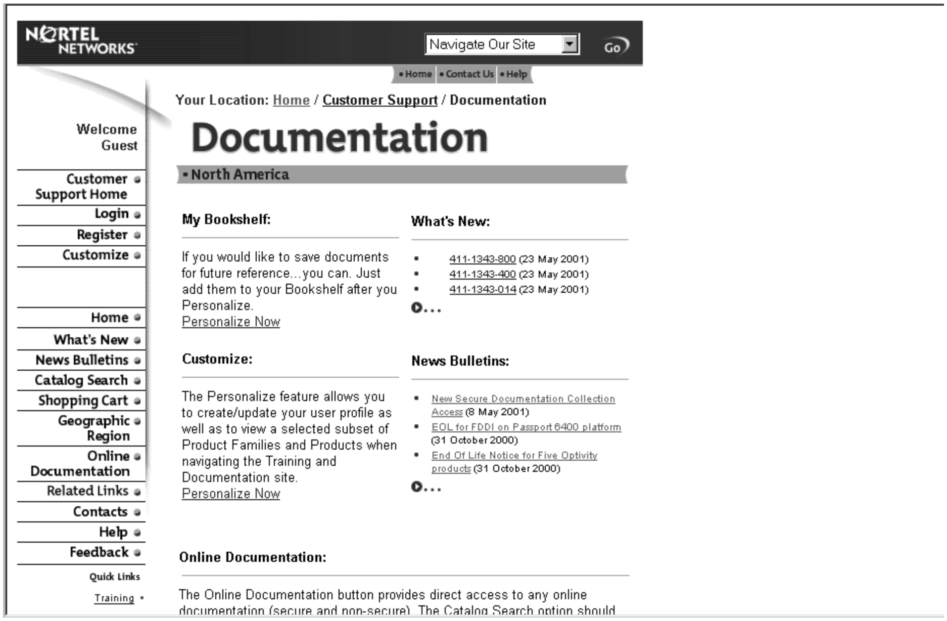
You can download current documentation about the Web-based management user interface from Nortel Networks Technical Documentation Web site.

To download current documentation:

1 From the main menu, choose Support > Release Notes.

Nortel Networks Technical Documentation Web site opens in a separate Web browser (Figure 176).

Figure 176 Nortel Networks Technical Documentation Web site


NORTEL NETWORKS
Navigate Our Site
Go
• Home • Contact Us • Help
Welcome Guest
Customer Support Home
Login
Register
Customize
Home
What's New
News Bulletins
Catalog Search
Shopping Cart
Geographic Region
Online Documentation
Related Links
Contacts
Help
Feedback
Quick Links
Training

Your Location: Home / Customer Support / Documentation

Documentation

• North America

My Bookshelf:

If you would like to save documents for future reference...you can. Just add them to your Bookshelf after you Personalize.
Personalize Now

What's New:

- 411-1343-800 (23 May 2001)
- 411-1343-400 (23 May 2001)
- 411-1343-014 (23 May 2001)

...

Customize:

The Personalize feature allows you to create/update your user profile as well as to view a selected subset of Product Families and Products when navigating the Training and Documentation site.
Personalize Now

News Bulletins:

- New Secure Documentation Collection Access (8 May 2001)
- EOL for FDDI on Passport 6400 platform (31 October 2000)
- End Of Life Notice for Five Optivity products (31 October 2000)

...

Online Documentation:

The Online Documentation button provides direct access to any online documentation (secure and non-secure). The Catalog Search option should

2 Locate your product, and click the document you want to download.

The BPS 2000 documentation is in the Data and Internet Product Family.

3 Click on the PDF icon to start the download process (you need Adobe Acrobat 3.0 or later to view or print documents from this site).

4 Follow the prompts to download the documentation.

5 Close the Web browser.

Upgrade option

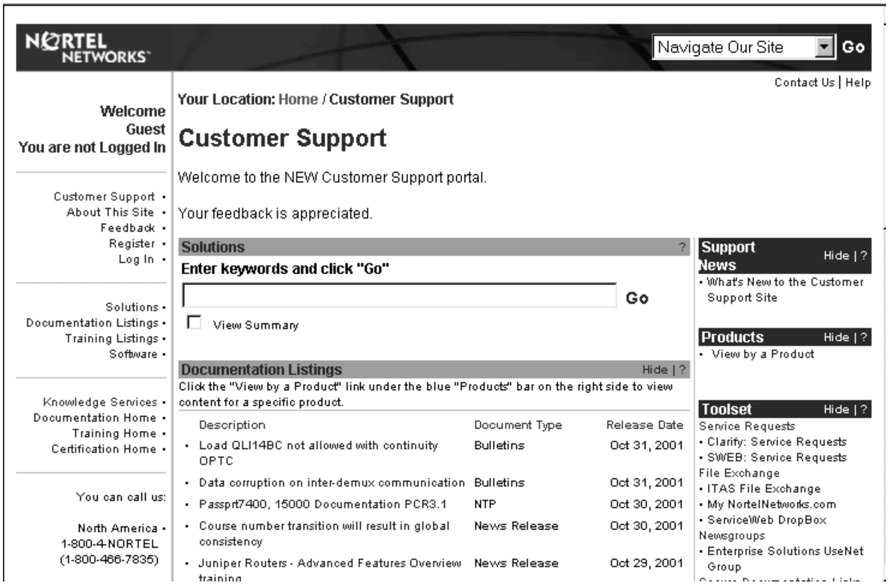
You can upgrade your Web-based management user interface to the most recent software release.

To upgrade to the most recent software release:

1 From the main menu, choose Support > Upgrade.

Nortel Networks Customer Support opens in a separate Web browser (Figure 177).

Figure 177 Nortel Networks Customer Support Web site


NORTEL NETWORKS
Navigate Our Site
Go
Contact Us | Help
Welcome
Guest
You are not Logged In
Customer Support •
About This Site •
Feedback •
Register •
Log In •
Solutions •
Documentation Listings •
Training Listings •
Software •
Knowledge Services •
Documentation Home •
Training Home •
Certification Home •
Solutions ?
Go
☐ View Summary
Documentation Listings Hide | ?
Support News Hide | ?
• What's New to the Customer Support Site
Products Hide | ?
• View by a Product
Toolset Hide | ?
Service Requests
• Clarify: Service Requests
• SWEB: Service Requests
File Exchange
• ITAS File Exchange
• My NortelNetworks.com
• ServiceWeb DropBox
Newsgroups
• Enterprise Solutions UseNet Group

Your Location: Home / Customer Support

Customer Support

Welcome to the NEW Customer Support portal.

Your feedback is appreciated.

Enter keywords and click "Go"

Click the "View by a Product" link under the blue "Products" bar on the right side to view content for a specific product.

Description	Document Type	Release Date
• Load QLI14BC not allowed with continuity OPTC	Bulletins	Oct 31, 2001
• Data corruption on inter-demux communication	Bulletins	Oct 31, 2001
• Passprt7400, 15000 Documentation PCR3.1	NTP	Oct 30, 2001
• Course number transition will result in global consistency	News Release	Oct 30, 2001
• Juniper Routers - Advanced Features Overview training	News Release	Oct 29, 2001

You can call us:

North America •
1-800-4-NORTEL
(1-800-466-7835)

2 Follow the prompts to download the software release.

3 Close the Web browser.

Refer to Chapter 4 for complete instructions on downloading software to a standalone BPS 2000, to a stack of pure BPS 2000, and to a mixed (Hybrid) stack.

Index

Numbers

450 Image Filename field 117

802.1p Assignment Table 262

802.1p Priority field 262, 264, 266, 267, 280, 285, 287

802.1p Priority Mapping page 263

802.1p Priority Queue Assignment page 261

A

Absolute Bandwidth field 255

access 94
- console 127
- number 48
- RADIUS security 47
- SNMP 94, 97
- Telnet 94
- TELNET/WEB/SNMP 30
- user levels 48
- Web 34

Accounting Time field 309

Action Creation 288

Action Name field 289

Action Table 288

Actions page 288

Active Phy field 115

Address Type field 312

administrative options 41
- CPU/memory utilization viewing 43
- logging on 47
- logging out 51
- resetting the switch/stack 49
- resetting to system defaults 50
- security, configuring
  - passwords 44
  - remote dial-in access 46
- system information, viewing 42

Administrative Status field 93

Administrative Traffic Control field 93

Agent page 304

Aging Time field 109

alarms 130, 133

Alias field 113

Alignment Errors field 154

Allow Packet Reordering field 306

Allowed Source field 103

Allowed Source IP field 96

Allowed Source Mask field 96

application setting options
- broadcast domains 188
- Common Open Policy Services (COPS) 308
- IGMP 167
- MultiLink Trunking 202
- port mirroring 162
- QoS 263
  - 802.1p priority queue assignment 261
  - actions 288
  - DSCP mapping 265
  - DSCP queue assignment 264
  - interface groups 254
  - IP filters 268
  - layer 2 filters 278
  - meters 291
  - network access 268
  - policies (hardware filters) 297

        Policy Agent (QPA) 304
        QoS Quick Config 236
        QoS Wizard 208
        role combination 254
        shapers 295
    rate limiting 165
    VLANs 173

Auth 311

Auth Failures field 311

Auth Missing ffield 311

Auth Type field 313

Authentication Password field 74

Authentication Protocol field 73

Authentication Protocols Supported field 71

Authentication Trap field 70

authentication traps, enabling 69

Authorization Type field 309

autonegotiation 111
    gigabit ports 114

Autonegotiation field 113, 115

autoPVID 30, 172, 188, 190

AutoPVID field 174

Autotopology 69

AutoTopology field 70

Available field 44

B

Bad Ctype field 310

Bad Sends field 311

Bandwidth Allocation field 255

Bandwidth field 255

bandwidth utilization 205, 255

BootP
    configuring 64
    request modes 65

BootP Request Mode field 65

BPS 2000 Diagnostics Filename field 117

BPS 2000 Image Filename field 117

Bridge Hello Time field 201

Bridge Information page 199

Bridge Priority field 194, 200

bridge settings 199

broadcast domains, configuring 188

Broadcast field 137, 141, 145

broadcast traffic 165

Burst Size field 296, 297

C

Capabilities field 259

Carrier Sense Errors field 154

Cascade Ports field 259

check boxes, about 39

Clear by Ports page 104

Clear Message From field 135

Client Type field 308, 312

Collisions field 137, 146

Comm Port Data Bits field 127

Comm Port Parity field 127

Comm Port Stop Bits field 127

Committed Burst Size field 292, 293

Committed Rate field 292, 293

Common Open Policy Services (COPS)
    sequential algorithm 313

Common Open Policy Services (COPS)
    about 307
    configuring 311
    deleting a client 314
    round robin algorithm 313
    statistics 309
    viewing capabilities and statistics 308

Community field 90

community strings, configuring 69

configuration file 124, 126

Configuration File Download/Upload page 124

Configuration Image Filename field 125
Configuration page 311
Console page 39, 45
Console Password Setting page 44
Console Port Speed field 127
Console Stack Password Type field 45
Console Switch Password Type field 45
Console/Communication Port page 127
conventions, text 26
conversation steering 162
COPS Capabilities field 308
Copy Configuration Image to Server field 125
CPU utilization 29, 43
CPU/Memory Utilization page 43
CRC Align Errors field 137, 141
Current Learning Mode field 99
Current Level field 131
Current Running Version field 117
customer support 28

D

DA Filtering on Intrusion Detected field 99
DA MAC Address field 107
DA MAC Filtering page 106
Data Specification field 293
Decryption Error field 72
Default Gateway field 66
default mapping 261, 263, 264, 265
default settings 50
Deferred Packets field 146
Deferred Transmissions field 155
Description field 54
Designated Root field 200
Destination Address field 270, 274, 276
destination address filtering 96
Destination Address Mask field 270, 274, 276
Destination IP L4 Port Max field 281
Destination IP L4 Port Min field 281
Destination IP L4 Port Range field 283
Destination L4 Port field 270, 274, 276
Destination L4 Port Max field 285, 287
Destination L4 Port Min field 285, 287
Display Message From field 135
Display Unit field 135
Download Option field 117
Drop 141
Drop Events field 136, 141
Drop Precedence field 266, 267
DSCP 276
  802.1p priority mapping 265
  mapping 263
  queue set associations 264
DSCP field 264, 265, 266, 267, 270, 271, 274, 276, 280, 285, 287
DSCP Mapping Modification page 265
DSCP Mapping page 265
DSCP Queue Assignment page 264

E

EAPOL Administrative State field 93
EAPOL Security Configuration page 91
EAPOL-based network security 30
EAPOL-based security 30, 91
Entry field 100, 103
Entry Storage field 73, 76, 79, 81, 83, 86, 88, 256
errors 148, 150, 153, 157
Ethernet error statistics
  viewing 153
  viewing in a bar graph format 156
  viewing in a pie chart format 155
Ethernet Errors
  Chart page 155

Ethernet Errors page 153
EtherType field 280, 285, 287
Excessive Collisions field 146, 149, 155
Extended Discipline field 255

F

fault threshold parameters, configuring 130
FCS Errors field 145, 149, 154
features 29
Filter Group field 300, 302
Filter Group Name field 274, 276, 285, 287
Filter Group Type 302
Filter Group Type field 300
Filter Tagged Frames field 189
Filter Unregistered Frames 189
Filter Untagged Frames field 189
Filtererd Packets field 145
Find MAC Address page 109
Flooded Packets field 145
Flow Control field 115
Forward Delay field 200, 201
Forward Delay Time field 194
Fragments field 137
Frame Errors field 145, 149
Frame Too Long field 154
From System Boot-Up field 44

G

gateway addresses, configuring 64
GBIC 30
General Discipline field 255
Generate SNMP Trap on Intrusion field 99
gigabit Ethernet 30, 114
Group Access Rights page 78
Group Creation page 193
Group Membership page 75
Group Name field 76, 79
Group page 202

H

hardware description 54, 56
Hello Interval 194
Hello Time field 194, 200
High Speed Flow Control page 114
high speed flow control, configuring 114
Host Address field 271
Hybrid Stack 32, 128

I

icons, about 39
Identify Unit Numbers page 62
IGMP Multicast Group Membership page 170
IGMP page 167
IGMP VLAN Configuration page 168
IGMP, configuring 167
In Discards field 151, 158
In Errors field 151, 309
In Frames field 158
In Non-Unicast field 151
In Octets field 151
In Packets field 309
In Unicast field 151
In Unknown Protos field 151
In-Band Stack IP Address field 66
In-Band Subnet Mask field 66
In-Band Switch IP Address field 66
Initialize field 93
In-Profile Action field 293, 300, 301
In-Profile Octets field 302
Interface chart field 151

Interface Chart page 152

interface class
  trusted, untrusted, and unrestricted 256, 259, 267

Interface Class field 256, 259

Interface Configuration page 254

Interface Direction field 300

Interface Group Assignment page 258, 259

Interface Group Creation 254

Interface Group Table 254

Interface ID page 257

Interface ID Table 257

Interface page 150

Interface Queue Table 254

interface statistics
  viewing 150, 151
  viewing in a bar graph format 152
  viewing in a pie chart format 152

Internal MAC Receive Errors field 154

Internal MAC Transmit Errors field 154

Interval field 132

In-Use field 66

IP address 64
  per unit 30, 64

IP Address field 54, 56, 90, 313

IP Classification Group page 273

IP Classification page 268

IP Filter Creation 268

IP Filter Group Table 268

IP Filter Table 268

IP gateway address 64

IP Group Modification page 275

IP manager list 30, 94

IP manager-based network security 30

IP page 64

IP Protocol field 281

ISVN numbers 119, 121

J

Jabbers field 137

K

Keep Alive Time field 309

L

Last 1 Minute field 44

Last 10 Minutes field 44

Last 10 Seconds field 44

Last 24 Hours field 44

Last 60 Minutes field 44

Last BootP field 66

Last Conn Attempt field 309

Last Error field 309

Late Collisions field 146, 149, 155

Layer2 Classification page 278

Layer2 Filter Creation 278

Layer2 Filter Group Table 278

Layer2 Group modification page 286

Layer2 Group page 284

Layer2Filter Table 278

Learn by Ports page 101

Learning Constraint field 174, 175, 177, 179, 183, 184, 186

LEDs 49, 50, 57, 62, 118

Length Mismatch field 310

Limit field 166

Link field 113, 149

Link/Trap field 113

Local Store Version field 117

logging on 47

logging out 51

Lost Packets field 145

LowMark field 44

M

MAC address 56

MAC Address field 54, 61, 103, 107, 109

Mac Address field 56

MAC Address page 186

MAC address security 97
  allowed source 102
  clearing 104
  deleting ports 105
  learn by ports 101
  learning 99
  MAC DA 30, 97, 106
  ports 104
  security list 99
  security table 102

MAC Address Security field 98

MAC Address Security SNMP-Locked field 98

MAC Address Table page 108

MAC address-based port mirroring 162, 164

MAC addresses
  locating a specific address 109
  viewing learned addresses 108

MAC DA filtering 96, 106

main menu
  headings and options 37
  icons 38, 40

Maintain Policing Statistics field 306

Management Information View page 80

Management VLAN field 174

Manufacturing Date Code field 54, 56

Max. Age Time field 194

Maximum Age Time field 200

Maximum Installed Instances filed 306

Maximum Message Size field 306

Maximum Requests field 93

MDA Description field 56

MDA field 54

MDAs 29, 30, 114

memory utilization 29, 43

Message field 135

Message Type field 135

Meter Creation 291

Meter field 300

Meter page 291

Meter Table 291

Meters page 293, 296

Microsoft Internet Explorer, software version requirements 33

mixed stack 30, 32

Module Description field 56

Monitor Port field 163

Monitoring 163

Monitoring Mode field 163

monitoring modes 164

Msg Processing Model field 88

multicast 167

Multicast field 137, 141, 145

Multicast Group Address field 170

multicast traffic 165

MultiLink Trunking 198
  about 202
  configuring 202
  monitoring traffic 205

Multiple Collision Frames field 155

Multiple Collisions field 146, 149

multiple spanning tree groups 30, 192

N

naming ports 113

Netscape Navigator, software version requirements 33

network access, configuring IP filters 268
Network Address field 270
network administrator
  contact information 67, 68
network monitoring 129
network security, protecting system integrity 35
new features 29
New Unit Number field 61
Not in Time Window field 72
Notification page 83
Notify Name field 83
Notify Tag field 83
Notify Type field 83
Notify View field 79
numbering
  ports 33
  stacks 60
  unit 33, 56, 60, 62

O

Octets field 136, 141
online help, accessing 315
Open Attempts field 310
Open Failures field 310
Operational State field 54, 56
Operational Status field 93
Operational Traffic Control field 93
Order field 274, 276, 285, 287
Out Discards field 151
Out Errors field 151
Out Frames field 158
Out Non-Unicast field 151
Out Octets field 151
Out Packets field 309
Out Profile field 303
Out Unicast field 151
Out-of-Profile Action field 300, 301
Out-Profile Action field 293
Overflow in Profile Octets field 303
Overflow Out Profile Octets field 303
Overflow Packet Hits field 302
Overflow Shaping Q Drops field 303
Oversize field 137, 141
Oversized Packets field 145

P

Packet Hits field 302
Packet Type field 166
Packets field 137, 141, 145
Packets length field 137, 145
Parameter field 131
Parameter Tag field 88
Participation field 198
Partition Port on Intrusion Detected field 98
Partition Time field 99
passwords, setting
  console 44
  remote dial-in access 46
  Telnet 44
  Web 44
Path Cost field 198
Permit field 270, 275, 277
physical view 57
PIDs 180
Policies page 298
Policy Class Name field 306
Policy Name field 300, 302
Policy Order field 300, 301
Policy Statistics page 301
Port
  Chart page 147
port autonegotiation speed

- configuring 111
- gigabit ports 114

Port Based modification page 176

Port Based page 175

port communication speed, configuring 127

Port Configuration page 104, 188, 197

Port Error Summary page 148

Port Information page 190

port list 33

Port List field 99, 100

Port List page 100

Port Lists page 99

Port Management page 111

Port Membership field 259

port mirroring 162

Port Mirroring page 162

Port Name field 189, 191

port naming 111, 113

port number 33

Port page 143

Port Priority field 190

port statistics 30
- viewing 143, 144, 148
- viewing in a bar graph format 147
- viewing in a pie chart format 147
- zeroing ports 146

Port/Port Membership field 177, 183

port-based port mirroring 162, 164

ports
- enabling 113
- naming 30, 113
- trusted, untrusted, and unrestricted 256, 267

power status 55

Power Status field 56

Preconfigured Port # field 271

Preferred Phy field 115

Primary RADIUS Server field 46

Priority field 198, 313

Private Protocol field 73

Private Protocols Supported field 71

product support 28

Protocol field 174, 179, 270, 271, 274, 276, 285, 287

Proxy field 167, 169

publications
- hard copy 27
- related 26

Pure BPS 2000 Stack 128

PVID 30, 188

PVID field 190, 191

Q

QoS 261, 263, 264, 265
- 802.1p priority mapping, configuring 263
- 802.1p priority, configuring 261
- about 253
- actions 288
- aggregate shaping 301
- bandwidth allocation 255
- burst size 291, 295
- capabilities 256
- committed rate 291, 295
- COPS 304, 307, 308
- data specification 291
- defined filters, installing 291, 297
- discipline 255
- drop precedence 265
- DSCP mapping, configuring 265
- DSCP queue set association, creating 264
- duration 291, 295
- entry storage 256
- Ethertype 278
- filter actions
  - about 288
  - deleting 290
- hardware filters
  - deleting 303
  - installing 298

  viewing statistics 301
ignore vlaue 269
in-profile action 298
interface class (trusted, untrusted, unrestricted) 256, 267
interface groups 254
  configuring 254
  deleting 260
  modifying 257
IP filter groups
  about 268
  configuring 272
  deleting 277
  modifying 275
IP filters
  about 268
  configuring 268
  deleting 272
layer 2 filter groups
  about 278
  configuring 284
  deleting 287
  modifying 286
layer 2 filters
  about 278
  creating 278
  deleting 283
loss sensitivity 267, 288
matching 268, 278
metered data 298
meters 30, 291, 298, 300
  deleting 294, 297
multiple VLANs 30, 278
no meter data 298
order 273
out-of-profile action 298
packet reordering 298, 304
policies 254
  configuring 291, 297
  disable 300
  enable 300
  statistics 301
policy server control 304
ports 254
  adding or removing 259
  type (trusted, untrusted, unrestricted) 256
  type (trusted, untrusted, untrestricted) 267
queue sets 261, 264, 306
  DSCP associations, creating 264
rate shaping 295
role combinations
  adding 259
  deleting 260
  modifying 257
  removing 259
service order 255
shaper groups 301
shaping 29, 295
statistics 298, 301, 304, 306
tagging 279, 281, 285
trusted ports 256, 267
unrestricted ports 256, 267
untrusted ports 256, 267
VLAN tagging 278
Wizard
  prioritizing traffic 212
  standard traffic 208

QoS Policy Agent Reset to Defaults field 305

QoS Policy Agent Retry Timer field 305

QoS Policy Agent State 305

QoS policy agent, configuring 304

QoS Policy Server Control field 305

QoS Quick Config 30, 236
  aggregate shaping 248
  filter groups 245
  interface class 237
  Interface Group page 237
  IP filters 241
  Layer 2 filters 243
  meters 247
  multiple VLANs 243
  policies 250
  Policy page 239
  port membership 237
  role combinations 237
  shaper groups 248

  - shapers 248
- QoS Wizard 29, 211
  - meters 211
  - prioritizing user defined traffic flows 226
  - prioritizing VLANs 213
  - proitizing IP applications 220
  - QoS Policies to Configure window 211
  - shapers 211
- Query Time field 168, 169
- Queue field 262, 265
- Queue Set field 262, 265
- Queue Sets field 258
- Queue Size field 296, 297
- Quiet Period field 93

R

- RADIUS page 46
- RADIUS Shared Secret field 47
- RADIUS-based network security 46, 91
- Rate field 296
- rate limiting
  - about 165
  - configuring 165
- Rate Limiting page 165
- Read View field 79
- Read-Only Community String field 70
- Read-Only Stack Password field 46
- Read-Only Switch Password field 45
- Read-Write Community String field 70
- Read-Write Stack Password field 46
- Read-Write Switch Password field 45
- Re-authenticate Now field 93
- Re-authentication field 93
- Re-authentication Period field 93
- redundancy 202
- Remote Access page 94
- remote dial-in access, configuring 46
- Reset page 49
- Reset to Defaults page 50
- resetting the switch/stack 49
- resetting the switch/stack, to system defaults 50
- Retrieve Configuration Image from Server field 125
- Retry Algorithm field 313
- Retry Count field 313
- Retry Interval field 313
- Rising Action 131
- Rising Level field 131
- RMON
  - Ethernet statistics
    - viewing 136
    - viewing in a bar graph format 138
    - viewing in a pie chart format 139
  - history statistics
    - viewing 140
    - viewing in a line graph format 142
- RMON Ethernet
  - Chart page 138
- RMON Ethernet page 136
- RMON Event Log page 133
- RMON History
  - Chart page 142
- RMON History page 140
- RMON options
  - fault event log, viewing 133
  - fault threshold parameters
    - configuring 130
    - deleting 132
  - history statistics
    - viewing 140
- RMON Threshold Creation field 132
- RMON Threshold page 130
- RMON, about 129
- Robust Value field 168, 169
- Role Combination field 256, 258, 259, 300, 301, 302

role combinations 254

Root Path Cost field 200

Root Port field 200

S

Sample/Alarm Sample field 132

Secondary RADIUS Server field 46

security 30, 91
  EAPOL-based 30
  IP manager list 30
  MAC address-based 97
  passwords 44
  RADIUS-based 46
  remote dial-in access 46
  SNMPv3 68, 70

Security Configuration page 97

Security field 105

Security Level field 79, 88

Security Model field 76, 79

Security Name field 76, 88

Security page 97

Security Table page 102

Select VLANs field 109

Serial Number field 54, 56

Server Timeout field 93

service class 211

Service Class field 266, 267

Service Order field 255

Set Drop Precedence field 290

Shaper Creation 295

Shaper field 300, 301

Shaper Group field 300, 301

Shaper page 295

Shaper Table 295

Shaping Q Drops field 303

Shaping Rate field 295

Single Collision Frame field 155

Single Collisions field 146

SNMP
  about 68
  MAC address security 98
  trap receivers
    configuring 89
    deleting 90

SNMP Engine Boot field 71

SNMP Engine Dialect field 71

SNMP Engine ID field 71

SNMP Engine Maximum Message Size field 71

SNMP Engine Time field 71

SNMP Trap Receiver page 89

SNMP/Access field 95

SNMP/Use List field 95

SNMPv1
  about 68
  configuring 69

SNMPv1 page 69

SNMPv3 70
  about 68
  configuring 70
  group access rights 78
    deleting 79
  group membership 75
    deleting 77
  management information views 80
    deleting 82
  system information, viewing 70
  system notification entries 82
    deleting 84
  target addresses 85
    deleting 87
  target parameters 87
    deleting 89
  user access 72
    deleting 75

Snooping field 167, 168

software
  downloading 116

- Hybrid Stack 119
- mixed stack 119
- upgrading 116, 121

software download
- LED indication descriptions 118
- process 116

Software Download page 116, 120, 122, 123

software upgrade 29, 317

Software Version field 54, 56

software version requirements
- Microsoft Internet Explorer 33
- Netscape Navigator 33

software versions 29, 30, 32, 43, 53, 116, 120, 121, 122, 123

Source Address field 270, 274, 276

Source Address Mask field 270, 274, 276

Source field 109

Source IP L4 Port Max field 281

Source IP L4 Port Min field 281

Source IP L4 Port Range field 283

Source L4 Port field 270, 275, 276

Source L4 Port Max field 286, 287

Source L4 Port Min field 285, 287

spanning tree 192
- bridge information 199
- learning mode 204
- learning modes 198
- port path cost 198
- port priority 198

Spanning Tree Add VLAN page 195

spanning tree configuration 197

spanning tree groups 30, 192
- adding VLANs 195
- bridge information 199
- configuring 193
- default 192
- number of 30, 32
- ports 197
- removing VLANs 195
- tagged BPDU 192
- tagging 192, 194, 201
- VLANs 195

spanning tree ports
- configuring 29, 197
- enabling 197
- FastLearning 197

Speed/Duplex field 114, 149

SQE Test Errors field 155

Stack Information page 53

stack information, viewing 53

Stack Numbering page 60

stack numbering, configuring 60

stack operational mode 50

Stack Operational Mode page 128

stack operational modes 128

stacking 30, 32, 50, 53, 60, 128, 171

Start field 141

Start TFTP Load of New Image field 117

State field 174, 198, 300

Static Router Ports field 169

statistics 30, 129, 138, 140, 142, 143, 146, 148, 153, 157

Status field 149

Status page 308

STGs 192

STP Learning field 204

Subnet Mask field 270

summary options
- changing stack numbering 60
- identifying unit numbers 62
- viewing
  - stack information 53
  - switch information 55
  - switch information in real time 57

Supplicant Timeout field 93

Support menu
- online help 315

  technical publications 316
  user interface, upgrading 317
support, Nortel Networks 28
switch configuration files
  requirements for retrieving 126
  requirements for storing 126
  TFTP server 124
switch images, downloading 116
switch information
  viewing 55
  viewing in real-time 57
Switch Information page 55
Switch View page 57
sysContact field 43
sysDescription field 43
sysLocation field 43
sysName field 43
System Contact field 68
system default settings, resetting to 50
System Description field 54, 68
System Information page 42, 48, 70
system information, viewing 42
System Location field 68
system location, naming 67
System Log page 134
system log, viewing 134
System Name field 68
system name, configuring 67
System Object ID field 68
system operational modes, configuring 128
System page 67
system settings
  modifying 67
  system contact 68
  system location 68
  system name 68
system statistics options, viewing
  Ethernet error statistics 153
  interface statistics 150
  port statistics 143
  QoS 301
  transparent bridging statistics 157
System Up Time field 68
sysUpTime field 43

T

tables and input forms, about 39
Tagged BPDU on Tagged Port field 194, 201
tagged frames 188
Tagged Trunk 190
tagged trunk 177
tagging 177, 188, 198
Tagging field 190, 198
Target Address field 86
Target Address page 85
Target Domain field 86
Target Name field 86
Target Parameter Entry field 86
Target Parameter page 87
Target Retry Count field 86
Target Tag List field 86
Target Timeout field 86
TCP Connection Attmepts field 310
TCP Connection Failures field 310
TCP Port field 308, 313
technical publications 27, 316
technical support 28
Telnet Password Setting page 44
Telnet/Access field 95
Telnet/Use List field 95
text conventions 26
TFTP
  configuration file 124

- server 124
- software download 124

TFTP Server IP Address field 117, 125

Time Stamp field 134, 135

Timeout Clients field 311

Total Octets field 145, 302

Total Overflow Octets field 302

Track Statistics field 300, 301

Traffic Type field 205

traffic, classifying 268

Transmit Period field 93

Transmit/Drop Frame field 289

Transparent Bridging
- Chart page 159

Transparent Bridging page 157

transparent bridging statistics
- viewing 157, 158
- viewing in a bar graph format 160
- viewing in a pie chart format 159

Trap Receiver Index field 90

traps 89

Triggered By field 134

troubleshooting 30
- access 94
- address filtering 96
- autonegotiation 111, 113
- configuration file 126
- COPS 313
- defaults 50
- gigabit ports 114
- LEDs 119
- MDAs 111
- memory 43
- mixed stack 32
- port speed 111
- QoS 208, 211, 254, 256, 261, 263, 264, 265, 268, 294, 298
- software upgrading 33, 116, 123
- spanning tree groups 32, 192, 197
- stacking 30, 59, 128
- VLANs 32, 171, 174, 178, 188, 197

Trunk field 198

Trunk Mode field 204

Trunk Name field 204

Trunk Port Members field 204

Trunk Status field 204

trusted ports 256, 259, 267

U

UDP RADIUS Port field 47

Unavailable Context field 72

Undersize field 137, 141

Undersized Packets field 145

Unit field 54, 56

unit number 33, 56, 60

unit numbers
- identifying 62

unit numbes
- numbering
  - units 54

Unknown Context field 72

Unknown Ctype field 310

Unknown Engine IDs field 72

Unknown Opcode field 310

Unknown User Name field 72

unregistererd frames 188

unrestricted ports 256, 259, 267

Unsupported Client Type field 310

Unsupported Security Level field 72

Unsupported Version field 310

Untagged Access 190

untagged access 177

untagged frames 188

untrusted ports 256, 259, 267

Update 802.1p Priority field 290

Update DSCP field 289

upgrades 29

User Defined Port # field 271

User Defined Protocol field 174, 179

user interface, upgrading 317

User Name field 73

User Specification page 72

Utilization page 205

V

VID used for Tagged BPDU field 194, 201

View Mask field 81

View Name field 81

View Subtree field 81

View Type field 81

VLAN Configuration
  MAC SA Based modification page 185
  MAC SA Based setting page 183
  Protocol Based modification page 182
  Protocol Based setting page 178

VLAN Configuration page 173

VLAN field 279, 287

VLAN Membership
  Add VLAN page 196
  Remove VLAN page 196

VLAN Membership page 195

VLAN Name field 174, 175, 179, 183, 184, 186, 191

VLAN Tag field 279, 281

VLAN Tag Required field 285, 287

VLAN Type field 174, 191

VLANs 30, 171
  about 171
  autoPVID 172, 174
  broadcast domains, configuring 188
  configuring 173
  deleting 188
  finding MAC addresses 109
  learned MAC addresses 108
  MAC SA-based
    about 172
    assigning MAC addresses 186
    configuring 183, 187
    deleting MAC addresses 187
  mixed stack 171
  number of 30, 32, 171
  port information
    viewing 190
  port-based
    about 172
    configuring 175
  protocol-based
    about 172
    configuring 178
    number of 172
    number of protocols 178
    reserved PID types 181
    supported PID types 180
  selecting a management VLAN 187
  STG 32
  tagging 279, 281, 285

W

Web browser, requirements 33

Web Page/Access field 95

Web Password Setting page 44

Web/Use List field 96

Web-based management interface
  home page, graphic 35
  logging in 34
  main menu, icons 38, 40
  management page 39
  navigating the menu 36
  requirements to use 33
  Web page layout 35
  Web page layout, graphic 36

Write View field 79

Wrong Digest field 72

Wrong Objects field 311

Wrong OpCode field 311